Regulation 910/2014/EU

Jacquemin, Hervé; Gillard, Noémie

Published in:
Concise European Data Protection, E-Commerce and IT Law

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

CHAPTER 9

Regulation 910/2014/EU – eIDAS Regulation

Hervé Jacquemin & Noémie Gillard[*]

[Text of the Regulation]

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

(Electronic Identification and Trust Services (eIDAS) Regulation)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee,[1]

Acting in accordance with the ordinary legislative procedure,[2]

Whereas:

(1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic

* Funded by the FEDER for the research project 'Wol-e-Cities'.

1. OJ C 351, 15 November 2012, p. 73.
2. Position of the European Parliament of 3 April 2014 (not yet published in the Official Journal) and decision of the Council of 23 July 2014.

interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

(3) Directive 1999/93/EC of the European Parliament and of the Council,[3] dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of that Directive.

(4) The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.

(5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6) In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.

(7) The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce,[4] stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.

(8) Directive 2006/123/EC of the European Parliament and of the Council[5] requires Member States to establish 'points of single contact' (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.

3. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19 January 2000, p. 12).
4. OJ C 50 E, 21 February 2012, p. 1.
5. Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27 December 2006, p. 36).

(9) In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.

(10) Directive 2011/24/EU of the European Parliament and of the Council[6] set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting 'common identification and authentication measures to facilitate transferability of data in cross-border healthcare'. Mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework.

(11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council.[7] In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

(12) One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.

(13) Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of all, some or

6. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4 April 2011, p. 45).
7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23 November 1995, p. 31).

none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.

(14) Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State's electronic identification scheme meets the conditions of notification and the notification was published in the *Official Journal of the European Union*. However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.

(15) The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.

(16) Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities. In particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technology-neutral. It should be possible to achieve the necessary security requirements through different technologies.

(17) Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member

States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties.

(18) This Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.

(19) The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be discussed and developed within the scope of the interoperability framework. Nevertheless technical requirements stemming from the inherent specifications of national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.

(20) Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.

(21) This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation cover aspects related to the conclusion and validity of contracts or

other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

(22) In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.

(23) To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.

(24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.

(25) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.

(26) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.

(27) This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

(28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided.

(29) In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC,[8] in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.

8. Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27 January 2010, p. 35).

(30) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.

(31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.

(32) It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users' trust in the single market.

(33) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.

(34) All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.

(35) All trust service providers should be subject to the requirements of this Regulation, in particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.

(36) Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of users and to the functioning of the internal market. Non-qualified trust service providers should be subject to a light touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of this Regulation.

(37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the

services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

(38) Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.

(39) To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).

(40) To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practice between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.

(41) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

(42) To facilitate the supervision of qualified trust service providers, for example, when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.

(43) In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment should be carried out by a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.

(44) This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council[9] which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.

(45) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services.

(46) Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.

(47) Confidence in and convenience of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly differentiate qualified trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.

(48) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC,[10] electronic signatures with a lower security assurance should also be accepted.

(49) This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.

(50) As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it

9. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13 August 2008, p. 30).
10. Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 274, 20 October 2009, p. 36).

is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.

(51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

(53) The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.

(54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.

(55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions

for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.

(56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.

(57) To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.

(58) When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.

(59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.

(60) Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.

(61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

(62) In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an

advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.

(63) Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.

(64) When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU.[11]

(65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.

(66) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services.

(67) Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum – CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

11. Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 53, 26 February 2011, p. 66).

(68) The concept of 'legal persons', according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.

(69) The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation capitalising, in particular, on existing good practices and the results of ongoing projects in the areas covered by this Regulation.

(70) In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(71) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[12]

(72) When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.

(73) For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.

(74) To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with

12. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28 February 2011, p. 13).

Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.

(75) The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.

(76) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(77) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council[13] and delivered an opinion on 27 September 2012.[14]

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

1. **Historical background.** Regarding the main principles governing the fulfilment of formal requirements by electronic means, reference must be made, at the international level, to the UNCITRAL Model Law on Electronic Commerce (1996), the UNCITRAL Model Law on Electronic Signatures (2001) and the United Nation Convention on the use of Electronic Communications in International Contracts (New York, 2005). At the European Union (EU) level, Directive 2000/31/EC states that 'Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means' (art. 9 (1)). Attention must also be paid to the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signature (OJ L 13, 19 January 2000). The scope of this directive is however limited to the sole formality of electronic signature.

2. **Weakness of the former legal framework and need of a new legislative initiative.** This legal framework at least deserves to exist, although one must admit that, in

13. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12 January 2001, p. 1).
14. OJ C 28, 30 January 2013, p. 6.

business practice, the use of electronic signatures with the higher level of security and legal certainty remains very low. In addition, some uncertainty remains, in the EU, with regard to numerous formalities (other than signature), which do not exist at the EU level (archiving, time stamping, registered letter, etc.). Some Member States took initiatives, but, with low harmonisation levels and, accordingly, a risk for the internal market. Considering that it could give rise to a lack of trust 'in particular because of a perceived lack of legal certainty, [that] makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services' (*see* recital 1 of the eIDAS Regulation), the European Commission issued a proposal for regulation in June 2012 (proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, COM (2012) 0238 final). A bit more than two years later (which is a pretty short period), this proposal was adopted: it is the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28 August 2014), also called the eIDAS Regulation. Compared to the 'directive', the regulation does not need to be implemented within the Member States. Such a legal instrument prevents potential differences between the legal frameworks applicable in the Member States, to the prejudice of the internal market (in any case when it is a minimal harmonization directive, but also when it is a maximal harmonisation directive, with the possible discussion on the scope of the directive – *see* the case Law of the CJEU with regard to Directive 2005/29/EC on unfair commercial practices). In point 1.5.3. of the proposal, reference was indeed made to the 'fragmented transposition and implementation of that Directive [1999/93/EC on electronic signature], which have blocked it from achieving its objectives'.

3. **Structure of the eIDAS Regulation and implementing acts.** The eIDAS Regulation is divided into two main chapters, dedicated to electronic identification (Chapter II) and Trust Services (Chapter III) and is supplemented by several implementing acts. Reference must also be made to Chapter I on 'general principles' (including the definitions), Chapter IV on 'electronic document', Chapter V on 'delegation of powers and implementing provisions' and Chapter VI on 'final provisions'. Four annexes must also be taken into account. They state the requirements for: (i) qualified certificated for electronic signatures; (ii) qualified electronic signature creation devices; (iii) qualified certificates for electronic seals; and (iv) qualified certificates for website authentication. The following implementing acts were also adopted (until 31 December 2017):

- The Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to art. 12 (7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- The Commission implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to art. 12 (8) of Regulation

(EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

- The Commission implementing regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to art. 8 (3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- The Commission implementing decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to art. 22 (5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- The Commission implementing decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to arts 27 (5) and 37 (5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- The Commission implementing decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to art. 9 (5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- The Commission implementing decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to arts 30 (3) and 39 (2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[Subject matter]

Article 1

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

(a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
(b) lays down rules for trust services, in particular for electronic transactions; and

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

1. General. This provision points out both the main objectives of the Regulation – proper functioning of the internal market and adequate level of security for electronic identification means and trust services – as well as the main measures adopted for this purpose – a new legal framework for electronic identification and trust services. Some rules – related to their legal effects – are also laid down for electronic documents (that are not, as such, trust services).

2. Objectives. (a) Trust, thanks to legal and technical certainty. The use of information and communication technologies (mainly internet) in electronic transactions is a source of economic growth. However, electronic transactions will not occur without a sufficient level of trust among the stakeholders (consumers, business and public authorities). This purpose is pointed out in recital 2 of the eIDAS Regulation: 'This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union'. Various threats to the establishment of a trust context can be outlined. Fraud and cybercrime are ubiquitous in the digital environment. Identity fraud and phishing, for instance, are common. The technical and legal security of the electronic transactions must be ensured. Pursuant to the applicable legal framework to be observed by the subjects of the eIDAS Regulation in the Member States, various formal requirements must be fulfilled. The requirements are for evidentiary purposes, tax purposes or aiming at protecting a weaker contract party (e.g., consumer) or a third party. In the digital context, where no handwritten signature can be included on a paper medium, in order to be further archived with the other paper records, one could wonder how to fulfil the main formalities, prescribed by the applicable legal framework (signature, in writing, handwritten mention, etc.) so that the electronic process used shall have equivalent legal effects to the corresponding 'paper' process. Further to these 'main' formalities, 'accessories' formal requirements also needed to be regulated: time-stamping, electronic registered delivery services or website authentication. For instance, in the context of a public procurement process, it could be required from the participant to demonstrate that the documents to be included in the tender were sent to, and received by, the public authority in compliance with the compulsory deadline. One could expect that archiving services would be regulated by the eIDAS Regulation as well. Unfortunately, this is not the case. The European regulator did not want to interfere with the archiving legal requirements enacted in each Member State. Member States remain free to regulate this service. For instance, the Belgian legislator introduced such regulation with the adoption of additional rules on electronic archiving, consistent with the principles and the logic laid down in the eIDAS Regulation. **(b) Ensuring the proper functioning of the internal market.** This objective is particularly

important in the context of information and communication technologies, where the services can easily be provided cross-border without any (technical) issue. The legal framework must therefore allow the provision of online services among the territory of the EU. By way of an example: a Swedish consumer must be able to use a trust service of electronic signature, provided by a Spanish provider, in order to conclude an agreement with a French company. From a *legal point of view*, this objective can only be achieved with a minimum set of harmonised rules within the Member States, with regard to electronic identification and trust services. This means that: (i) all trust services must be regulated (and not only the electronic signature, such as in the Directive 1999/93/EC) and (ii) the level of harmonisation must be as high as possible, in order to prevent from differences among the Member States. This is the reason why the European legislator decided to adopt a regulation, directly applicable in the Member States and with low – however not inexistent – margin left to derogate from its provisions (and not a minimal harmonisation directive). With reference to the Directive 1999/93/EC on electronic signature, recital 3 states that it 'dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of that Directive'. From a *technical point of view*, it is also critical that the interoperability of the identification schemes and the trust services is ensured. By way of an example: a Belgian citizen should be able to use his electronic identity card in order to authenticate with a French public administration or when applying online in to Italian University. For these purposes, common technical norms must be established – and accepted in the Member States –, in order to allow the systems available in the States to 'communicate' with each other, in accordance with the best security standards.

3. Means adopted in order to achieve the objectives. In order to achieve these objectives, three means are referred to in art. 2 of the eIDAS Regulation. They deal with electronic identification (section a) and with trust services (section b). The first means are regulated in Chapter II of the eIDAS Regulation (art. 6-12) and the other means in Chapter III (art. 13-45). Both measures are strongly linked to each other (e.g., the relation between the electronic signature and the electronic identification are pretty obvious) but they could also be regulated by distinct texts at the EU level. However, the European Commission chose to take up the challenge to include both subjects in a single regulation.

[Scope]

Article 2

> **1. This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.**
>
> **2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.**

> **3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.**

1. General. This provision determines the scope of the eIDAS Regulation, from a positive (*it applies to ... – cf.* art. 2 (1) -) and a negative (*it does not apply to ...* – cf. art. 2 (2) and 2 (3) -) perspective. A distinction must also be made whether the scope limitation refers to electronic identification, trust services, or both. In any case, the scope is pretty broad (there are only few limitations). The broad scope allows any party to rely on the Regulation in the public sector (especially for e-government issues) or in the private sector, no matter whether it concerns a B2B, a B2C or a C2C relationship, with cross-border dimension or not.

2. Scope defined positively. (a) Application to notified electronic identification schemes. Para. 1 of art. 2 states: 'this Regulation applies to electronic identification schemes that have been notified by a Member States'. Art. 6-12 of the eIDAS Regulation determine the legal framework applicable to electronic identification. The legal framework applies to the identification schemes subject to a notification, in accordance with the procedure laid down in art. 9 (1) of the Regulation. It means, in other words, that the Member States establishing such identification schemes remain totally free to decide whether to notify (and be subject to the duties prescribed by the Regulation, as well as by the rights, in particular the mutual recognition consecrated in art. 6 or not. **(b) Application to trust service providers established in the Union.** Following para. 1 of this provision, the Regulation only applies to trust service providers established in the Union. This is consistent with the internal market principle, consecrated in art. 4 of the Regulation (*see* comment below). Trust services could nevertheless be provided to customers (consumers or professionals) located in the Union by providers established outside the Union (for instance, in the United States or in India). Such providers remain free to decide whether they will comply with the requirements of the eIDAS regulation or not. Their customers will not benefit from the protection rules laid down in the Regulation setting up a high level of legal certainty. However, it is possible, under art. 14 of the eIDAS Regulation (and its corresponding requirements), to recognise a trust service provider established in a third country as being legally equivalent to qualified trust service providers established in the Union.

3. Scope defined negatively. (a) Not applicable to closed systems. Pursuant to art. 2 (2), the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants are excluded from the scope of the Regulation. Additional details are given in recital 21 of the Regulation, stating: '[f]or example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation'. This limitation appears to be pretty logical: in closed systems where, normally, the parties know each other (and where their main rights and duties are laid

down in an agreement), they could freely decide not to use a (qualified) trust service provided by a (qualified) trust service provider and to grant legal effects to a trust service that does not meet the requirements prescribed by the eIDAS Regulation. This is an application of their contractual freedom. This freedom is however not absolute: it cannot give rise to the violation of a mandatory legal provision, that shall be observed in a specific situation. For instance, in accordance with point (q) of Annex of the Directive 93/13/EEC of the Council on unfair terms in consumer contracts, the following terms may be regarded as unfair: terms which have the object or effect of 'unduly restricting the evidence available to [the consumer] or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract'. Furthermore, when the mandatory legal framework prescribes a signature or a written agreement as a requirement to the validity of the contract (in order to protect consumers, for instance), parties cannot rely on the scope limitation of art. 2 (2) of the eIDAS Regulation in order to use an electronic signature process with lower level of security. **(b) Rules related to the conclusion and validity of contracts not affected.** Art. 2 (3) of the eIDAS Regulation states that it: 'does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form'. A distinction must be made between, on the one hand, the formal requirement as such, prescribed by national or Union Law and related to the conclusion and validity of contracts (written and signed agreement prescribed for evidentiary purposes, for instance, or as mandatory requirement, whose violation could allow a termination of the agreement or any other penalty), and, on the other hand, the rules to be observed in order to fulfil this formal requirement in the digital context, so that it can benefit from the same legal effects (as in the 'paper' context). The Regulation applies only to these last aspects. The Member States remain free to impose specific legal requirements and to determine their purpose (and corresponding penalty in case of violation). Recital 21 also specifies that the Regulation: 'should not affect national form requirements pertaining to public registers, in particular commercial and land registers'.

[Definitions]

Article 3

For the purposes of this Regulation, the following definitions apply:

(1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

(2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

(3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

(4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

(5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

(6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;

(7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

(8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council;[15]

(9) 'signatory' means a natural person who creates an electronic signature;

(10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;

(12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

(13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;

(14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

(15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

(16) 'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
(b) the creation, verification and validation of certificates for website authentication; or
(c) the preservation of electronic signatures, seals or certificates related to those services;

(17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;

15. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28 March 2014, p. 65).

(18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

(19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

(21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;

(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;

(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;

(24) 'creator of a seal' means a legal person who creates an electronic seal;

(25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

(26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;

(27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

(28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;

(29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

(30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

(31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;

(32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

(33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;

(35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

(36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(37) 'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44;

(38) 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

(39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

(40) 'validation data' means data that is used to validate an electronic signature or an electronic seal;

(41) 'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.

1. Electronic identification. The process of electronic identification is intended to allow for online identification of a person, thanks to the use of personal identification data in electronic form (art. 3 (1)). These data must be uniquely linked to the person seeking identification, who can be either a natural or legal person, as well as a natural person representing a legal person. The personal identification data is contained in electronic identification means, which can either be material medium or an immaterial unit (art. 3 (2)). e.g., the Belgian electronic ID card serves as an electronic identification means, as it contains two certificates, including one for identification purposes. The sole presentation of personal identification data is not self-sufficient. In order to access an online service, the link between the personal identification data and the natural or legal person has to be confirmed through an authentication process. Thanks to this authentication process, the relying party will be able to know, with a high level of certainty, the identity of the person seeking access. The electronic identification means are part of what is called an electronic identification scheme, which is described as 'a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons' (art. 3 (4)). As explained below, Member States have the faculty – but not the obligation (recital 13) – to notify their national electronic identification schemes to the Commission in order for them to appear on a list of electronic identification schemes, and provided that a number of requirements are fulfilled (arts 7 and 9). If all the requirements are met, the inscription of the national electronic identification scheme triggers the application of the mutual recognition principle (recital 14 and art. 6).

2. Electronic signature. The electronic signature is created by a person, called the 'signatory', to whom the signature is uniquely linked. The signatory must be necessarily a natural person, as legal persons use another tool: the electronic seal. This will be explained in the next paragraph. Under the Regulation, three types of electronic

signature emerge. First, the 'simple' electronic signature is defined in art. 3 (10), as 'data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign'. This constitutes the basis of the criteria that every electronic signature must fulfil. The definition does not give much information about the electronic signature and, basically, revolves around the act of signing. The Member States determine what is meant under this expression. The second defined form of an electronic signature is the 'advanced' electronic signature (art. 3 (11)). Compared to the simple electronic signature, the advanced electronic signature must fulfil additional requirements enumerated in art. 26 of the Regulation. From those requirements, the advanced electronic signature should derive a strengthened level of security and, correlatively, enhanced trust from the relying parties. At the top of that security scale stands the 'qualified' electronic signature (art. 3 (12)). Additionally to the criteria linked to the advanced electronic signature, the qualified electronic signature must be created using a qualified electronic signature creation device. It must be based on a qualified certificate for electronic signature. A certificate for electronic signature is an 'electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person' (art. 3 (14)). In order to be qualified, this electronic document has to be issued by a qualified trust service provider. Furthermore, it must meet several requirements listed in Annex 1 to the Regulation (art. 3 (15)). As for the electronic identification device, art. 3 (22) defines it as a 'configured software or hardware used to create an electronic signature'. If this device meets the requirements enumerated in Annex II, it is called a qualified electronic identification device. The electronic signature is constructed on the basis of electronic signature creation data, defined as 'unique data which is used by the signatory to create an electronic signature' (art. 3 (13)).

3. Electronic seal. The electronic seal is an electronic tool destined to be created and used by a legal person, who is known as the 'seal creator'. As is the case with the electronic signature, three models of electronic seals are provided for in the Regulation. The 'simple' electronic seal is defined as 'data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity' (art. 3 (25)). This definition is very similar to the definition of the electronic signature, the main difference being that the functions of the electronic seal – guaranteeing the origin and integrity of the data – are specifically mentioned, while art. 3 (10) merely indicates that the electronic signature is used by the signatory 'to sign'. The 'advanced' electronic seal must meet the requirements laid down in art. 36 (art. 3 (26)). The 'qualified' electronic seal is an advanced electronic seal which is created with a qualified electronic seal creation device and which is based on a qualified certificate for electronic seals (art. 3 (27)). Those three types of electronic seals are therefore built on the same foundations as the three models for an electronic signature.

4. Trust services (provider) and qualified trust service (provider). In the context of trust services an important distinction is made between qualified trust service and a qualified trust service provider, on the one hand, and a non-qualified trust service and

non-qualified trust service provider, on the other hand. The definition of trust service is lay down in art. 3 (16) of the Regulation. First, it is considered as an 'electronic service normally provided for remuneration'. This concept – normally provided for remuneration – is also used in art. 57 of the Treaty on the Functioning of the EU, as well as in various other regulations (*see* for instance the definition of 'information society service', in the E-Commerce Directive 2000/31/EC). Following the interpretation given by the European Court of Justice, an information society services is a service that must be provided for economic purposes, no matter whether the price is paid directly by the recipient of the service or is resulting from the advertising revenues gained by the provider. Three kinds of services are referred to in the definition: the first two references describe the trust services regulated by the Regulation: '(a) creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services' or '(b) the creation, verification and validation of certificates for website authentication'. The third services references to archiving, as it related to '(c) the preservation of electronic signatures, seals or certificated related to those services'. Any trust service can be qualified or non-qualified. Should a trust service be qualified then, in accordance with the definition, it shall meet 'the applicable requirements laid down in this Regulation' (art. 3 (17) of the Regulation). Qualified trust services are subject to numerous requirements (compared to non-qualified trust services, for which only few requirements are applicable). Correlatively, with the legal effects of qualified trust service, the relying parties should benefit from a higher level of legal certainty. Trust service providers and qualified trust service providers are also defined by the Regulation (*see* art. 3 (19) and 3 (20) of the Regulation).

5. (Qualified) Electronic time stamp. The definition of electronic time stamp is built with reference to the functions of the process. The electronic time stamp process does not have an equivalent in the 'paper' environment. It means 'data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time' (art. 3 (33) of the Regulation). A distinction is made between the electronic time stamp and the qualified electronic time stamp. The last one shall meet the requirements of art. 42 of the Regulation (art. 3 (34) of the Regulation – *see* comment at art. 42 of the Regulation).

6. Electronic document. A broad definition of the 'electronic document' is given under art. 3 (35) of the Regulation. It is 'any content stored in electronic form'. Some examples are provided: 'text or sound, visual or audio-visual recording'. It is not limited to the written form. An electronic document is not a trust service. It shall however benefit from the principle of non-discrimination, like the other trust services (*see* art. 46 of the Regulation). On the principle of non-discrimination, *see* below, in particular the comments of arts 25 and 46.

7. (Qualified) Electronic registered delivery service. The electronic registered delivery service is defined in art. 3 (36) of the Regulation, with reference to the functions of the corresponding process in the 'paper' environment: transmission of data between third parties; proof of sending and receiving the data; protection of data against risk of

loss, theft, damage or any unauthorized alterations. A distinction is made between the electronic registered delivery service and the qualified registered delivery service that shall meet additional requirements, prescribed in art. 44 of the Regulation.

8. (Qualified) Certificate for website authentication. The certificate for website authentication t is understood as 'an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued' (art. 3 (38) of the Regulation). This trust service aims at preventing the risks of phishing, notably in the financial sector. Such certificate could be non-qualified or qualified and, in this last case, the requirements of Annex 4 shall be met.

[Internal market principle]

Article 4

> **1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.**
>
> **2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.**

1. General. As soon as a trust service provider is established in a Member State of the Union and provided it complies with the rules prescribed by the eIDAS Regulation, it is allowed to provide its trust services in the territory of any other Member States, without any restriction. For example, a Greek public authority could not impose prior notification to a non-qualified trust service provider of a non-qualified electronic signature, established in Croatia, willing to grant its (non-qualified) trust services to the Greek market. This internal market principle is closely related to the country of origin principle, as referred to in art. 3 of the E-Commerce Directive (*see* comment of the provision). Once authorized in a Member State (and considered as a qualified trust service provider, for instance), no more authorization can be requested from such provider before it can provide its trust services in another Member State. Otherwise, the objective of proper functioning of the internal market would not be achieved. As specified in para. 2 of the provision, products and trust services shall be permitted to circulate freely in the internal market. Reference is made to both 'trust services' a 'products'. Products are defined as 'hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of services' (art. 2 (21) of the eIDAS Regulation). In other words, the internal market principle thus provides for free circulation, applicable not only to the trust service as a whole, but also to its hardware or software components.

2. Specific rules applicable to qualified trust services. In compliance with the internal market principle, a qualified trust service issued in a Member State shall be recognised as a qualified trust service in all other Member States (*see* art. 25 (3) for qualified electronic signature; art. 35 (3) for qualified electronic seals and art. 41 (3) for

qualified electronic time stamp). It is however not consecrated for qualified electronic registered delivery service or qualified certificates for website authentication.

[Data processing and protection]

Article 5

> **1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.**
>
> **2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.**

1. General. In most cases, the provision of electronic identification systems and trust services will involve the processing of personal data. It is obvious that the rules regarding the processing of personal data are applicable and that these must be observed. As of 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data is applicable. Directive 95/46/EC was repealed as that same date. Hence, the wording in the first paragraph is no longer accurate. A broader reference would have made more sense and it is likely that this paragraph must be amended.

2. Pseudonyms. Art. 5 (2) expressly excludes any prohibition of the use of pseudonyms in electronic transactions. In other provisions of the eIDAS Regulation, especially in the context of electronic signature, the Regulation allows the reference to a pseudonym of the signatory, instead of the name (*see*, in particular, the definition of 'certificate for electronic signature' in art. 3 (14) of the Regulation). Recital 33 states however that 'provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law'.

CHAPTER II

ELECTRONIC IDENTIFICATION

[Mutual recognition]

Article 6

> **1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:**

(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;
(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;
(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

1. General. This provision aims at handling an issue mentioned in recital 9 of the eIDAS Regulation: 'In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States'. In order to take down this 'electronic barrier', art. 6 establishes the principle of mutual recognition. The mutual recognition of electronic identification schemes is intended to facilitate cross-border interactions between public authorities and citizens. If a Member State decides to notify an electronic identification system to the Commission, and provided that the three cumulative conditions established in this provision are met, the other Member States are under a positive duty to recognize it. Within twelve months after publication of the electronic identification scheme in the list provided for in art. 9 (the notification itself is subject to the conditions set forth in art. 7), the Member States must recognize said scheme.

2. Three cumulative conditions (para. 1). For this clause to be applicable, three cumulative conditions, described below, must be satisfied. **(a) Electronic identification is required under national law or administrative practice.** Electronic identification, using electronic identification means and authentication, must be required under the national law or administrative practice of the Member State providing online public services. Consequently, a Member State that allows access to online public services without requiring user's authentication does not have to comply with the obligation of mutual recognition. In practice, this is not problematic: if the public service is offered with free access, it is not necessary to use an electronic identification process, and even less so to have this process recognized. Hence the Regulation would not apply to this situation. **(b) Notification and publication.** The Member State in question must notify the electronic identification scheme to the Commission in order to be included in the list published by the Commission pursuant to art. 9. This notification itself is subject to compliance with several conditions listed in art. 7. **(c) Assurance levels.** The other conditions for the mutual recognition of the electronic identification scheme relate to assurance levels. recital 16 of the Regulation clarifies what must be understood under the concept of 'assurance level': 'The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (e.g., identity proofing and verification, and authentication), management activities (e.g., the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented.' Assurance levels are described in art. 8 of the Regulation. Pursuant to para. 3 of this provision, the Commission has adopted the Commission implementing Regulation (EU) 2015/1502 of 8 September 2015 setting out minimum technical specifications and procedures for assurance levels for electronic identification means. The assurance level attached to the electronic identification means must be equal or superior to the level attained for the online public service. More specifically, the obligation of mutual recognition only applies to electronic identification means that correspond to the assurance level substantial or high (*see* recital 15 of the Regulation). This highlights the importance for the electronic identification systems and trust services of attaining a high level of reliability, which is central to the objective of strengthening the trust of the European citizens in the electronic environment.

3. Voluntary recognition (para. 2). Recognition of an electronic identification means which correspond to the security level 'low' does not result in an obligation for a Member State to apply mutual recognition. However, when such an electronic identification means is issued under an electronic identification scheme that appears on the Commission's list, public sector bodies can voluntarily decide to recognize it and authorize access to the online service they provide through this means. We can safely presume that only a Member State that requires an assurance level 'low' in order to access an online public service would decide to recognize an electronic identification means corresponding to the assurance level 'low'. It is indeed highly unlikely that a public sector body would content itself with an electronic identification means that only match the criteria of the assurance level 'low', when its online service requires an assurance level 'substantial' or 'high'.

4. Member States' margin of manoeuvre. Mutual recognition is only imposed as regards cross-border authentication of online services. Consequently, the Regulation leaves it to the Member States to decide on the rules governing all other aspects of online services, notably conditions to access the service, its content, or the way it is provided.

[Eligibility for notification of electronic identification schemes]

Article 7

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

(a) the electronic identification means under the electronic identification scheme are issued:
(i) by the notifying Member State;

(ii) under a mandate from the notifying Member State; or
(iii) independently of the notifying Member State and are recognised by that Member State;

(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;

(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.
For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.
Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

(g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);

(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

1. General. Member States can notify electronic identification schemes to the Commission on a voluntary basis (recital 13 of the Regulation). Notification on a voluntary basis is subjected to a significant number of conditions that contribute to achieving the main purpose of the Regulation, namely the strengthening of trust through a high level of security.

2. Conditions. (a) Issuance of electronic identification means (art. 7, (a)). Three categories of actors can carry out the issuance of the electronic identification means: the Member State itself, an operator appointed by the Member State, or an independent

operator, provided that the electronic identification means are recognized by the Member State. A distinction must be made between 'notification', which is always performed by the notifying Member State, and 'issuance' of electronic identification means, which can be carried out by a private entity. This would be particularly relevant if the notifying Member State establishes that a private entity is already using electronic identification means which is eligible as regards the notified scheme. This participation of the private sector is mentioned in recital 13 of the Regulation, according to which '[Member States] should also be able to decide whether to involve the private sector in the provision of those means'. **(b) Utilization of the electronic identification means for access to at least one online public service.** The regulation requires that it should be possible to use the electronic identification means provided under the electronic identification scheme in order to access an online service offered by a public sector body and which necessitates electronic identification in the notifying Member State. The underlying idea is that the reliability of an electronic identification means can be presumed when the notifying Member State uses this means to provide access to its own public services at national level. This requirement contributes to generating other Member States' trust in the electronic identification means. **(c) Fulfilment of the requirements of at least one of the assurance level set out in the Regulation.** Only electronic identification schemes that correspond to the assurance levels 'low', 'substantial' or 'high' are eligible for notification. It must be emphasized that, while electronic identification means that correspond to the assurance levels 'substantial' or 'high' must be recognized by other Member States, electronic identification means which show 'low' assurance level do not fall under the obligation of mutual recognition. Those will be recognized only if Member States decide to do so (*see* art. 6 (2)). **(d) Personal identification data.** As regards personal identification data, the Regulation requires two things. First, the personal identification data must uniquely represent the person in question. In other words, an electronic identification means must correspond to only one person. The reverse is not true, as a person can have multiple electronic identification means. In such a case however, all the electronic identification means must link to the same person. This requirement aims at guaranteeing that a person using electronic identification means to prove his or her identity is indeed who he or she claims to be. Second, these data must be attributed to the person in accordance with the technical specifications, standards and procedures for the relevant assurance level, at the time the electronic identification means under the notified scheme is issued. This second – technical – aspect is specified in the Commission implementing Regulation (EU) 2015/1502 of 8 September 2015. **(e) Compliance with technical specifications, standards and procedures for the relevant assurance level when issuing the electronic identification means.** The entity that issues the electronic identification means to the targeted person must comply with technical specifications, standards and procedures for the relevant assurance level. This obligation is further specified in the aforementioned Commission implementing Regulation (EU) 2015/1502. This instrument aims at ensuring reliability and quality of the mechanisms involved in every aspect of electronic identification. **(f) Availability of online authentication.** As a counterpart to the recognition of a notified identification scheme, the notifying Member State must provide for means of online authentication (art. 7, (f),

sub-para. 1). The explanatory memorandum specifies that 'the authentication must be available without interruption' (*see* the Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market of 4 June 2012, COM (2012) 238 final). This authentication requirement is of utmost importance, considering that, as stated in the explanatory memorandum, '[t]he reliability of an electronic identification depends on the availability of means of authentication (i.e. the possibility to check the validity of the electronic identification data)'. For example, when a person uses its electronic identity card to access an online service, it must be possible to verify that this person is the rightful holder of the identity card. As the authors will see when examining art. 11, the notifying Member State will be held liable if online authentication is unavailable and a damage arises thereof, when the unavailability is intentional or due to negligence. The obligation is only imposed on the notifying Member State when the relying party established on another Member State's territory is a public sector body that offers an online service. Thanks to this authentication means, the public sector body will be able to verify the identity of the foreign user who wants to access the online service. In this situation, cross-border authentication is offered for free (art. 7, (f)). By contrast, in the hypothesis of an online service not offered by a public sector body, the obligation of providing online authentication that is normally imposed on the notifying Member State does not apply. The notifying Member State therefore regains its freedom to decide under which conditions the authentication can be accessed. For example, if a Dutch insurance company allows Belgian citizens to access its online services using their electronic ID card, Belgium can decide to charge the Dutch company for the verification of the ID card. Lastly, the notifying Member State must refrain to impose disproportionate technical requirements on relying parties, in such a way that interoperability would be jeopardized (art. 7, (f), al. 3). **(g) Communication of a description of the electronic identification scheme six months prior to the notification.** The Member State that intends to notify an electronic identification scheme must provide a description of this scheme to the other Member States at least six months before notification. This requirement is meant to make it possible for Member States to cooperate on the interoperability of not only notified but also soon-to-be notified electronic identification schemes (*see* art. 12, para. 5, of the Regulation). **(h) Compliance with the requirements set out in the implementing act.** In order to be eligible for notification, the electronic identification scheme must comply with the requirements set out in the implementing act adopted by the Commission as regards the interoperability framework. On 8 September 2015, the Commission adopted the implementing Regulation (EU) 2015/1501 on the interoperability framework pursuant to art. 12 (8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9 September 2015). Prior to this date, and the date of adoption of every implementing act provided in the Regulation, notification was not possible. Since 28 September 2015, all implementing act came into effect and notification is therefore possible.

[Assurance levels of electronic identification schemes]

Article 8

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Electronic identification means must be defined by reference to one out of the three assurance levels provided for by the Regulation. They can either show an assurance level low, substantial or high, each of these levels corresponding to particular technical specifications, standards and procedures which define what degree of reliability can be expected from electronic identification means. Recital 16 states: 'The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented.'

2. Relevance as regards mutual recognition and interoperability. Art. 8 (1) requires the notifying Member State to specify, in the notified electronic identification scheme, the assurance level attached to the electronic identification means under that scheme. Besides giving an idea as to the reliability of those electronic identification means, such a specification is particularly relevant in the context of mutual recognition and interoperability. First, Member States are under the obligation of mutual recognition only when the electronic identification means issued under an electronic identification scheme notified by another Member State corresponds to the assurance level low or high (art. 6 (1) sub-para. (b)). As regards the assurance level low, Member States do not have to recognize the electronic identification means, but they can do so on a voluntary basis (art. 6 (2)). Second, the requirement provided in art. 8 (1), is relevant for the obligation of interoperability. Indeed, an important part of the interoperability framework consists in minimal technical requirements related to the assurance levels established by the Regulation, and to a mapping of national assurance levels to the assurance levels under the Regulation (art. 12 (4)). The indication of the assurance level attached to an electronic identification means therefore helps positioning these means on the scale defined by the interoperability framework.

3. Criteria applying to each assurance level (para. 2). Art. 8 (2) describes each of the assurance levels by referring to the degree of confidence in the claimed or asserted identity of a person it implies. The assurance level low provides a limited degree of confidence in this regard, while the assurance levels substantial and high are the vectors of gradually higher degrees of confidence. As stated before, assurance levels are characterized with reference to particular technical specifications, standards and procedures. This technical framework is intended, in the context of assurance level substantial, to (substantially) decrease the risk of misuse or alteration of the identity. As for the assurance level high, its technical characteristics must erase the risk of misuse or alteration of the identity.

4. Obligation of the Commission (para. 3). The Commission must adopt implementing acts in order to establish minimum technical specifications, standards and procedures that apply to each assurance level. It must do so in light of pre-existing international standards, and taking into account the degree of confidence which must be achieved by the assurance levels. The technical characteristics of these assurance levels encompass every aspect the procedure followed for the issuance of the electronic

identification means – verification of the applying person's identity, issuance mechanism itself, issuing entity and involved body –, the authentication mechanism, and the technical and security specifications of the issued electronic identification means. Those implementing acts must be adopted in accordance with the comitology procedure. As the Commission completed its task, those minimum technical specifications, standards and procedures can be found in the Commission implementing Regulation (EU) 2015/1502 of 8 September 2015.

[Notification]

Article 9

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

(a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;

(b) the applicable supervisory regime and information on the liability regime with respect to the following:
  (i) the party issuing the electronic identification means; and
  (ii) the party operating the authentication procedure;

(c) the authority or authorities responsible for the electronic identification scheme;

(d) information on the entity or entities which manage the registration of the unique person identification data;

(e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;

(f) a description of the authentication referred to in point (f) of Article 7;

(g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Notification is always carried out by a Member State, as opposed to the issuance of electronic identification means, which can be taken care of by another entity (art. 7, (a)). Art. 9 requires the notifying Member State to provide a range of information about the electronic identification scheme, and changes that might occur. The provision establishes a framework for publication and amendments in the list of the notified electronic identification schemes.

2. Required information (para. 1). Art. 9 adds to the conditions stated in art. 7 by requiring the notifying Member State to provide a range of information about the electronic identification scheme that it intends to notify. Any change that results in this information becoming obsolete must be communicated without undue delay. This imposes an obligation on the notifying Member State to be transparent about each aspect of the notified electronic identification schemes. The information to be provided covers: a description of the electronic identification scheme – including its assurance levels and the issuer or issuers of electronic identification means –, the supervisory and liability regimes, authority or authorities responsible for the electronic identification scheme, entity or entities which manage the registration of the unique person identification data, a description of how the requirements on interoperability are met, a description of the authentication and arrangements for suspension or revocation in case of security breach. The notifying Member State must also provide information related to the party issuing the electronic identification means and the party operating the authentication procedure (para. 1, (b), (i) and (ii)), which will be relevant as regards distribution of liabilities in the case of damage (art. 11).

3. Publication and amendments (paras 2–4). On 8 September 2015, the Commission adopted its Commission implementing Regulation (EU) 2015/1502 – which sets out minimum technical specifications, standards and procedures for assurance levels – and its Commission implementing Regulation (EU) 2015/1501 on the interoperability framework (*see* above, in the Commentary of art. 7). One year from the date of application of those instruments, a list of the notified electronic identification schemes, alongside with the information thereon, was to be published by the Commission in the Official Journal of the EU (para. 2). After the expiry of this period, any new notification must be subject to an amendment to this list, within two months from the date of receipt of this notification (para. 3). Finally, a notifying Member State may request the removal from the list, of an electronic identification scheme that it notified. In this situation, the Commission benefits from a period of one month from the date of receipt of this request to proceed to the removal.

4. Circumstances, formats and procedures of notifications (para. 5). The Commission is entitled to adopt implementing acts in order to define the circumstances, formats and procedures of notifications. Contrary to the implementing acts referred to in art. 8, paras 3 and 12, paras 7 and 8, this provision only consists in an opportunity for the Commission, which is therefore not compelled to take such measures. However,

if the Commission decides to adopt those acts, it must do so through the comitology procedure. On the 3 November 2015, the Commission adopted an implementing decision (EU) 2015/1984 defining the circumstances, formats and procedures of notification.

[Security breach]

Article 10

> **1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.**
>
> **2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.**
>
> **3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.**
>
> **The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 9(2) without undue delay.**

1. General. In addition to mutual recognition, the successful notification by a Member State of an electronic identification scheme generates two other consequences. First, it generates a set of obligations that applies in the event of a security breach. The notion is not defined in the Regulation. An application of the concept can be found in the GDPR, under the notion of 'personal data breach', which defines a security breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4 May 2016). The second additional consequence of the notification of an electronic identification scheme is the application of a liability framework which is discussed in the Commentary on art. 11.

2. Positive obligations for the notifying Member State in case of a security breach (para. 1). Should the notified electronic identification means or authentication be breached or compromised, two obligations arise. First, the notifying Member State suspends or revokes, without undue delay, the cross-border authentication or its compromised parts. Second, the notifying Member States informs other Member States and the Commission of the incident. The notifying Member State decides whether the

cross-border authentication is suspended or revoked, depending on the level of gravity of the security breach. We should highlight the fact that the Regulation only provides revocation or suspension when, and to the extent that, the reliability of the cross-border authentication of the electronic identification scheme is put in jeopardy. If the impact of the security breach is purely national, the notifying Member State is free to react as it sees fit. In the same vein, national use of a breached or compromised electronic identification scheme is left at the discretion of the notifying Member State.

3. Two contemplated situations. (a) The breach or compromise is remedied within three months of the suspension or revocation (para. 2). In the event of a positive outcome, achieved within a three-month period, the notifying Member State re-establishes the revoked or suspended cross-border authentication and informs the Commission and other Member States of such a re-establishment. **(b) The breach or compromise is not remedied within three months of the suspension or revocation (para. 3).** Conversely, if the Member State fails to remedy the breach or compromise within three months, the consequence is the notification to the Commission and other Member States of the withdrawal of the jeopardized scheme. Without undue delay, the Commission formalizes the withdrawal through a modification of the list containing the notified schemes. This puts an end to the obligation of mutual recognition previously imposed on other Member States.

[Liability]

Article 11

> **1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.**
>
> **2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.**
>
> **3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.**
>
> **4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.**
>
> **5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.**

1. General. This clause aims at establishing the rules surrounding liability pursuant to the obligations set forth in art. 7. In the event that a successful notification is made, then the rules determining the allocation of liability between three types of actors come into play. Art. 11 regulates the potential liability of the actors mentioned in paras 1–3,

whose liability depends on the function they perform in the cross-border transaction giving rise to a damage event – whether notifying the electronic identification scheme, issuing the electronic identification means or operating the authentication procedure. It is noticeable that the Regulation establishes liability for damage caused 'intentionally or negligently'. The scope of liability will therefore be determined through the test of intent or negligence of the Member State or service provider. The seriousness of the violation is of no relevance, just as the concept of wilful misconduct.

2. Allocation of liability. (a) Liability of the notifying Member State (para. 1). The notifying Member State is liable for damage caused by a failure to comply with its obligations under the Regulation (art. 7, (d) and (f)). This clause provides a damages compensation remedy should the Member State (intentionally or negligently) fail to ensure that the personal identification data uniquely represent a person, and that these data are attributed in compliance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act (namely the Commission implementing Regulation (EU) 2015/1502 of 8 September 2015). Liability of the Member States for intentional failure to comply is not unusual in EU regulation but there is no competence for the European Court to decide on or impose any damages award (*see also* para. 4). The notifying Member State must also ensure the availability of online authentication, its free access when cross-border authentication is carried out in relation to a public service, and refrain from imposing any technical requirement that would be disproportionate and likely to harm interoperability. If the notifying Member State fails to fulfil one of these obligations, then it will incur liability for any damage that arises from such failure. **(b) Liability of the party issuing the electronic identification means (para. 2).** Failure of the issuing party make sure that the electronic identification means is delivered to the person to which the relevant personal identification data are attributed can result in liability for damages accruing as a result of such failure. **(c) Liability of the party operating the authentication procedure (para. 3).** The party operating the authentication procedure must ensure the correct operation of the authentication. As for the wording on 'correct operation' of the authentication, the Regulation does not specify what is meant precisely. The wording does not clarify how the correctness of the management should be assessed either. Therefore, the cases in which the liability of the operating party would be involved remain quite obscure and, as a consequence, difficult to enforce. At most, it can be inferred from the explanatory memorandum, which mentions 'security good practices'. A trust service provider would therefore be liable when he is negligent and fails to comply with those security good practices, or if this non-compliance is intentional.

3. National rules on liability (para. 4). Art. 12 specifies that national rules on liability will be applicable as regards responsibilities deriving from paras 1–3. This means that the definition and assessment of damages, the rules on civil procedure and the rules related to determining the burden of evidence – e.g., both as regards the damage causing event and the evidence of the damages suffered) continue to be governed by national law (*see* recital 18).

4. Scope of the regime. (a) Cross-border transactions. The allocation of liability as provided by this provision only apply in the event of a damage occurring in a cross-border context. If a national transaction gives rise to a damage, the liability regime is left to the discretion of the Member States. **(b) Liability regime limited to aspects of the transaction mentioned in art. 11 (para. 5).** In addition to the scope of the regime, the rules laid down in art. 11 only cover the aspects of cross-border transactions that are listed in paras 1–3, namely notification of an electronic identification scheme by a Member State, issuance of the electronic identification means, and management of the authentication procedure. Otherwise – content or execution of the transaction –, national law is applicable. **(c) Fragmentation of responsibilities.** It is likely that the lack of harmonization in this area will lead to a 'liability puzzle' and cause unwelcome difficulties when it comes to determining who is responsible in the case of damage. Moreover, it is likely that in some situations, the party issuing the electronic identification means will be different from the one operating the authentication procedure. Considering the complexity inherent to the field of electronic identification, it will often be tricky to identify the exact cause of a damage and, consequently, the responsible actor.

[Cooperation and interoperability]

Article 12

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.

2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:

(a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;
(b) it follows European and international standards, where possible;
(c) it facilitates the implementation of the principle of privacy by design; and
(d) it ensures that personal data is processed in accordance with Directive 95/46/EC.

4. The interoperability framework shall consist of:

(a) a reference to minimum technical requirements related to the assurance levels under Article 8;
(b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;
(c) a reference to minimum technical requirements for interoperability;
(d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;
(e) rules of procedure;
(f) arrangements for dispute resolution; and
(g) common operational security standards.

5. Member States shall cooperate with regard to the following:

(a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and
(b) the security of the electronic identification schemes.

6. The cooperation between Member States shall consist of:

(a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;
(b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;
(c) peer review of electronic identification schemes falling under this Regulation; and
(d) examination of relevant developments in the electronic identification sector.

7. By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.

8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.

9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Art. 12 is a central piece of this chapter. It is crystal clear that the imposition of obligations related to mutual recognition is vain if it is not accompanied by the technical circumstances making it possible for national systems to communicate.

2. Performance obligation (paras 1–4). The short wording of paras 1 and 2 of art. 12 does not leave much room for doubt as to the nature of the content they introduce. Para. 1 reads as follows: 'The national electronic identification schemes notified pursuant to art. 9 (1) shall be interoperable.'; while para. 2 states that in order to ensure the interoperability objective, 'an interoperability framework shall be established'. It is a real obligation of performance that is generated through this article, which applies to the Member States as well as to the Commission. **(a) Criteria to be fulfilled by the interoperability framework.** Para. 3 sets out the criteria that must be met by the interoperability framework. The framework must aim at technology neutrality and must not favour nor disadvantage any specific national technical solution (art. 12 (3) sub-para. (a)). This is one aspect of the technology neutrality principle that is outlined in recital 27 as one of the basic principles that governs the Regulation. The interoperability framework should also, when possible, apply international and European

standards (art. 12 (3) sub-para. (b)). The last two criteria relate to privacy and data protection (art. 12 (3) sub-paras (c) and (d)). Thus, the interoperability framework should facilitate the implementation of the principle of privacy by design. This principle means that when building new systems, whether technical or legal, a focus should be put on privacy from the first steps of their development. Moreover, the interoperability framework must ensure conformity with Directive 95/46/EC as regards data processing activities. In this sense, recital 11 states that 'authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online'. The Directive 95/46/EC has been replaced since then, by the General Data Protection Regulation of 27 April 2016. **(b) Content of the interoperability framework.** Para. 4 provides for a list of elements that should be contained in the interoperability framework, which are: 'a reference to minimum technical requirements related to the assurance levels under Article 8', 'a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8', 'a reference to minimum technical requirements for interoperability', 'a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes', 'rules of procedure', 'arrangements for dispute resolution' and 'common operational security standards'.

3. Obligations applying to Member States (paras 5 and 6). Art. 12 (5) and (6) define the lines along which the Member States should cooperate in order to achieve interoperability. The cooperation obligation targets not only the interoperability of the notified electronic identification schemes (art. 12 (5) sub-para. (a)), but also the security of the electronic identification schemes (art. 12 (5) sub-para (b)). For efficiency reasons, this also applies to electronic identification schemes that Member States intend to notify in the future. In this respect, art. 7 (g) provides that six months prior to notification, the notifying Member State should communicate to other Member States a description of the electronic identification scheme that it wants to notify. In practical terms, cooperation implies that Member States must exchange information, experience and good practice as regards every aspect of electronic identification schemes. Moreover, the required cooperation between Member States encompasses peer review of electronic identification schemes and examination of relevant developments in the electronic identification sector (art. 12 (6). Such sharing of knowledge can contribute to enhancing the assurance levels and, consequently, improve the quality of the tools and procedures used by operators throughout the EU.

4. Obligations applying to the Commission (paras 7 and 8). As set out in art. 12 (8) the Commission has the obligation to adopt implementing acts in order to lay down uniform conditions which would constitute a basis for interoperability. Those uniform conditions will materialize in the interoperability framework. In doing so, the Commission must conform to the criteria set out in para. 3, meaning it should ensure technological neutrality and avoid discrimination between Member States, strive to follow international and European standards and be protective of privacy and personal data. The Commission fulfilled its obligation by adopting the Commission implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework

(*see* above, in the Commentary of art. 7). Art. 12 (7) imposes on the Commission to pass other implementing acts, designed this time to set out procedural rules in order to regulate relationships between Member States. The Commission also carried out this task through the adoption of the Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to art. 12 (7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Para. 9 requires the respect of the comitology procedure for the adoption of those implementing acts.

CHAPTER III

TRUST SERVICES

SECTION 1

General provisions

[Liability and burden of proof]

Article 13

> **1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.**
>
> **The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.**
>
> **The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.**
>
> **2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.**
>
> **3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.**

1. General. If a trust service provider, whether qualified or non-qualified, violates one of its obligations under the Regulation, then this provider could be held liable and any natural or legal person affected by the violation, is entitled under this article to claim compensation of all or part of damages resulting from such failure. The person claiming damages could be the signatory or the user of the trust service, or any other person. As was the case in art. 11 (1), this provision requires that the trust service provider must have caused the damages either 'intentionally or negligently'. Art. 13 is without prejudice to right of the trust service providers to contractually limit their liability. For the application of the rules prescribed by paras 1 and 2 of this provision, reference is made to the national rules of liability. It means for instance that national law shall be

applicable in order to interpret the concepts of 'intention' or 'negligence', assess whether other liability requirements are fulfilled (damages, causal relationship, etc.) or determine the validity of any clause excluding or limiting the liability of the provider.

2. Burden of proof. The requirements to comply with in order to provide qualified trust services are numerous. Compared to the requirements applicable to non-qualified trust service providers they are particularly stringent for the provider. The stringency of the rules is offset somewhat by the requirement that the relying party of a qualified trust service will benefit from a higher level of legal certainty, resulting from such service (compared to a non-qualified trust service, with lower level of legal certainty). This higher level of legal certainly is, among other benefits, resulting from the burden of proof, in the case of intentional or negligent failure. (a) **Qualified trust service.** With a qualified trust service, the burden of proof – and the corresponding risk of a lack of proof, with the potential loss of the lawsuit –, relies on the qualified trust service provider. Its intention or negligence is indeed presumed, being agreed that it is allowed to demonstrate that the damage occurred without such intention or negligence. (b) **Non-qualified trust service.** In the case of a non-qualified trust service, the burden of proof lies on the natural or legal person claiming the damage. Should he/she/it fail to demonstrate that the damages were causes intentionally or negligently due to a failure to comply with the eIDAS Regulation, the claim will be judged ungrounded and no indemnification will be granted. In the present matter, the technical aspects are pretty complex to deal with, which increase the burden and the risks for the claimant.

3. Possible limitations of liability. As was stated under 2, the trust service provider may contractually impose a limitation of liability. Such a clause is subject to a double duty of transparency. First, the customers of the trust service provider must be duly informed in advance of such limitation. Second, such limitations must be recognisable to third parties. Subject to both requirements, the limitation of liability is valid and the provider shall not 'be liable for damages arising from the use of services exceeding the indicated limitations'. The trusted service provider could, for instance, impose a cap of EUR 10,000 of 50,000 for any damage occurring in an electronic transaction where a trust service was used in failure of the Regulation's duties. It is highly recommended to the providers to establish such limitation of liability, in line with their professional insurance.

[International aspects]

Article 14

> **1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.**

> **2. Agreements referred to in paragraph 1 shall ensure, in particular, that:**
>
> **(a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;**
>
> **(b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.**

1. General. In accordance with art. 2 (1), the Regulation applies to trust service providers established in the Union. As a matter of principle, trust service providers established in a third country are not subject to the requirements of the Regulation. Conversely, their trust services shall not benefit from the recognition of legal effect embedded in the Regulation either. Nevertheless, in the event the trust services providers fulfil some of the specific requirements enacted by art. 14, then their trust services could be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union. Art. 14 requires that the Union shall conclude an agreement with a third country or an international organization in accordance with art. 218 TFEU, stating such recognition of the trust service originating from third country. Art. 14 (2) adds two points that shall be governed by the agreement: (1) the trust service provider and its services meet the requirements of the Regulation applicable to the qualified trust service providers and their qualified services, and: (2) by virtue of mutual recognition principle, the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent in the third country or in the international organisation.

[Accessibility for persons with disabilities]

Article 15

> **Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.**

1. General. This duty of accessibility for persons with disabilities is usual in various other regulation at the EU level. As mentioned in recital 29 of the Regulation, it is in line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27 January 2010, p. 35),

in particular art. 9 of the Convention. It is only a duty of means for the provider ('where feasible'). Technical and economic considerations shall be taken into account, among other aspects, in the feasibility assessment.

[Penalties]

Article 16

> **Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.**

1. General. **In addition to the liability regime set forth in arts 11 and 13, this article** impose an obligation on the Member States to lay down effective, proportionate and dissuasive penalties in case of infringements to the rules of the Regulation. Such an obligation is pretty usual under EU Law (*see* for instance art. 20 of the E-Commerce Directive or art. 24 of the Consumer Rights Directive). Such penalties are necessary to ensure that the rules prescribed by the eIDAS Regulation will be respected by the actors that are subject to the regulatory requirements. Although this delegation to the Member States is not disputable per se, the main weakness lies in the potential differences between the national regulations, with a risk of competition between them. Some providers could indeed make the choice of their establishments in a Member State rather than in another one ('forum shopping'), in order to benefit from a less stringent legal framework (with regard to the penalties). Furthermore, it is important to state that such penalties will remain useless without the implementation of process and the allocation of sufficient resources allowing the competent authorities in the Member States to search for the infringements and to sue them. On this point, reference must also be made to the role and the competences of the supervisory body established in the Member States (on this point, *see* below the comment of art. 17 of the Regulation).

2. Example of penalties. There could be criminal, administrative or civil penalties applicable to the providers that do not comply with the eIDAS Regulation or any other provision enacted in the Member States in order to complement the Regulation. Civil penalties aim at protecting private interests of the relying parties and any user of the trust services. Member States shall appreciate whether the provision of specific civil penalties is appropriate. General rules applicable to Contracts or Torts could indeed be sufficient to achieve this goal. Criminal and/or administrative penalties shall be mobilized in order to protect the public interest. In this context, such penalties could for instance prohibit the activities of a trust service provider that does not comply with the applicable legal framework. Trust service providers alleging that they are qualified (although they are not) could also be condemned to pay a dissuasive fine.

SECTION 2

Supervision

[Supervisory body]

Article 17

> **1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State.**
>
> **Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.**
>
> **2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.**
>
> **3. The role of the supervisory body shall be the following:**
>
> **(a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;**
> **(b) to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.**
>
> **4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:**
>
> **(a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;**
> **(b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);**
> **(c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);**
> **(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;**
> **(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);**
> **(f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;**
> **(g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;**
> **(h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body;**

(i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);
(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).

7. The Commission shall make the annual report referred to in paragraph 6 available to Member States.

8. The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. The eIDAS Regulation lays down the rights and duties of the trust service providers, as well as the requirements applicable to them and to their services (being agreed that the legal framework is much more stringent for the qualified trust service providers): data protection, security requirements, competence of the supervisory body and, for qualified trust service providers, additional requirements, with prior authorisation and audit every twenty-four months, etc. Trust of the citizens, businesses and public authorities will not be ensured, if they have any doubts regarding the compliance with the requirements prescribed by the eIDAS Regulation, by the providers (and especially the qualified trust service providers). In order to achieve the goal of trust, the trust service providers are subject to the supervision of a public body designated by the Member States. As stated in recital 36 of the Regulation, 'Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of users and to the functioning of the internal market'. Art. 17 determines their designation, as well as their role and tasks in the context of trust services.

2. Designation of the supervisory body. Art. 17 (1) of the eIDAS Regulation regulates the designation of the supervisory body. This competence lies with the Member States. Normally, they should designate a body established on their territory. However, smaller States could cooperate and designate, upon mutual agreement, a supervisory body established in another Member State. Art. 17 (1) expressly requires that they: 'shall be given the necessary powers and adequate resources for the exercise of their task'. It must be stressed again that the main purpose of the eIDAS Regulation is to ensure a high level of trust among all the stakeholders. In this context, the role of the supervisory body is a key element to achieve this goal. Should the supervisory body be

unable to perform its tasks of control and take the necessary actions, because of a lack of powers or resources, the all system will collapse. Names and addresses of the supervisory bodies shall be communicated by the Member States to the Commission. In France, the supervisory body is the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI – https://www.ssi.gouv.fr/en/); in Belgium, it is the Federal Public Service Economy, S.M.E.s, Self-employed and Energy (www.economie.fgov.be), etc.

3. Role of the supervisory body. The role of the supervisory body will vary according to whether the trust service provider is qualified or non-qualified; should the trust service provider be qualified and established in the territory of the corresponding Member State, then the supervisory body shall be competent, in accordance with art. 17 (3) (a): 'to ensure, through *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation'. Its role *ex ante* lies in the prior authorization to be granted to the qualified trust service providers, before the initiation of their activities, in accordance with art. 21 of the eIDAS Regulation. Its *ex post* supervision is regulated by art. 20 of the Regulation. When the trust service provider is non-qualified, the supervision is 'subject to a light touch' (*see* recital 36). This is pretty logical since the requirements applicable to such providers remain basic, with a correlative low level of legal certainty for the services. The common ground between the qualified and non-qualified trust service providers lies in the fact that they are subject to *ex post* supervision. This supervision is limited to events where there is a necessity to take action. The necessity to act is determined based on information that those (non-)qualified trust service providers or the trust services they provide allegedly violate the requirements laid down in the eIDAS Regulation (art. 17 (3) (b) of the eIDAS Regulation). The *ex post* supervision is further detailed in art. 19 of the eIDAS Regulation. There is no general obligation to supervise the non-qualified trust service providers: information could be given by another supervisory body, any user or business partner or, the provider itself (*see* recital 36). Although there is no general duty to control the providers, the supervisory body is allowed to carry out its own investigations.

4. Tasks of the supervisory body. The main tasks of supervisory body are listed in art. 17 (4) of the eIDAS Regulation. Some of the tasks deal with the supervisory body's duty to cooperate with other supervisory bodies in accordance with their obligation of mutual assistance, as further detailed in art. 18 of the Regulation (*see* littera a). Such cooperation is particularly important should any breach occurs: for this purpose, some tasks refer to the duty to 'inform other supervisory body and the public about breaches of security or loss of integrity in accordance with Article 19 (2)' (*see* littera c) or 'to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data rules appear to have been breached' (*see* littera f). Other tasks are closely related to the supervision of the qualified trust service providers, *ex ante* and *ex post*: they deal with the duty to 'grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20

and 21' (*see* littera g); 'to inform the body responsible for the national trusted list referred to in art. 22 (3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body' (*see* littera h); 'to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1)' (*see* littera b) and 'to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20 (2)' (*see* littera e). Specific attention must be paid to one of the most important duties relying on the qualified trust service provider, related to the effect of the termination of its activities. The supervisory body must, in this context, 'verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24 (2)' (*see* littera i). The objective is 'to ensure sustainability and durability of trust service providers and to boost confidence in the continuity of trust services' (*see* recital 41 of the Regulation). Both qualified and non-qualified service providers can be subject to *ex post* control by the supervision body and, in this context, one of the tasks of the supervisory body is to 'require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation' (littera j).

5. Report to the EU Commission. Supervisory bodies shall produce a report at the end of each calendar's year, describing their main activities, together 'with a summary of breach notifications received from trust service providers in accordance with Article 19 (2)'; this report shall be submitted to the Commission by 31 March each year (*see* art. 17 (6) and art. 17 (5), littera d). Format and procedure for the report can be defined by the Commission (art. 17 (8)). These reports is further made available to the Member States by the Commission in accordance with art. 17 (7) of the Regulation.

6. Trust infrastructure. In accordance with art. 17 (5), Member States are entitled 'to require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law'.

[Mutual assistance]

Article 18

> **1. Supervisory bodies shall cooperate with a view to exchanging good practice.**
>
> **A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.**
>
> **2. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:**
>
> **(a) the supervisory body is not competent to provide the requested assistance;**
> **(b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;**

> **(c) providing the requested assistance would be incompatible with this Regulation.**
>
> **3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.**

1. General. As with most harmonization initiatives, the Regulation aims at ensuring the proper functioning of the internal market. Any EU citizen, business or public authority should be entitled to use the trust service offered by a provider (either qualified or not) established in another Member State and, therefore, controlled by the supervisory body of this Member State. In this context, the need of mutual assistance between the supervisory bodies seems obvious. The object of this provision is to determine the duties of the bodies with regard to this mutual assistance, as well as the implementation of joint investigations between several supervisory bodies.

2. Rights and duties of the bodies. The first purpose of the cooperation organized between the supervisory bodies is the exchange of good practices. It is important to ensure that, for instance when granting the qualified status, the practices are harmonized and as consistent as possible. Assistance could also be requested, with due justification, by a supervisory body, from a supervisory authority in another Member State. This could occur, for instance, in the case of 'information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21' (*see* art. 18 (1) of the Regulation). The supervisory body receiving such request shall normally answer positively, except if it can rely on one of the grounds referred to in art. 18 (2) of the Regulation: its incompetence to provide the requested assistance (a), the lack of proportionality of the requested assistance with regards to the tasks granted to the role and the tasks of the supervisory body pursuant to art. 17 of the Regulation (b) or the incompatibility of the requested assistance with the Regulation.

3. Joint investigation. In some cases, supervisory bodies of distinct Member States may consider appropriate to carry out joint investigation on a trust service provider. This may be authorised by the Member States, which shall also agree upon and establish the arrangements and procedures for such actions, in accordance with art. 18 (3) of the Regulation.

[Security requirements applicable to trust service providers]

Article 19

> **1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to**

prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

4. The Commission may, by means of implementing acts:

(a) further specify the measures referred to in paragraph 1; and
(b) define the formats and procedures, including deadlines, applicable for the purpose of paragraph 2.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Art. 19 of the eIDAS Regulation lays down the main security requirements applicable to the trust service providers. It must be stressed that it is applicable to both qualified and non-qualified trust service providers. It is therefore a key provision of the Regulation, since it is the only provision prescribing obligations to the non-qualified trust service providers. Depending on the trust service, the qualified trust service providers must comply with additional requirements, as described in art. 24, and with other provisions in the Regulation. The requirements deal with the technical and organisational measures to be taken by the providers and their notification duties, should a breach of security or a loss of integrity occurs. According to para. (4), implementing acts shall be adopted by the Commission in the context of this provision. At the time of writing, no security measures regulation had been enacted.

2. Technical and organisational measures. Appropriate technical and organisational measures must be taken by the trust service providers, pursuant to art. 19 (1) of the Regulation. It is an open norm and, to determine precisely the measures to be implemented, reference must be made to the latest technological developments and to the degree of risks. Such measures must indeed prevent and minimise the impact of security incidents.

3. Notification in the case of breach of security or loss of integrity. In line with the GDPR and other EU regulations, a notification process is organized by art. 19 (2) and (3) of the Regulation, should a breach of security or a loss of integrity occur. The provision is similar to the art. 33 GDPR (*see also* recital 85 GDPR). Both public authorities and natural or legal persons affected by such incident must be informed about the security incident. The ratio for this requirement being that these parties must be enabled to take the necessary measures in order to further protect public interests or safeguard their legitimate private interests (*see also* recital 38 of the eIDAS Regulation). Such notification duty applies both to qualified and non-qualified trust service providers. It is paramount that the duty is performed as quickly as possible. As regards notification to the supervisory body (and to any other relevant body, such as the data protection authority, in accordance with the applicable data protection law), notification must be made 'without undue delay but in any event within twenty-four hours after having become aware of it'. When the disclosure of the breach of security or loss of integrity is in the public interest, the notified supervisory must further inform the public. It could also require the trust service provider to do so, at its own costs. Trust services may be provided regardless of national borders between the Member States. Consequently, the breach of security or loss of integrity could concern two or more Member States. In that case, the supervisory body of such Member States, as well as ENISA (European Union Agency for Network and Information Security), shall be informed by the notified supervisory body. ENISA shall also be provided once a year, by the supervisory bodies of the Member States, 'with a summary of notification of breach of security and loss of integrity received from the trust service providers'. The objective is to 'enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation' (recital 39). The aforementioned process is only applicable to any breach of security or loss of integrity 'that has a significant impact on the trust service provided or on the personal data maintained therein'. In most cases, natural or legal persons will also be impacted by the incident and adversely affected by it; trust service providers shall therefore notify them without undue delay (the period of twenty-four hours is however not applicable here). This could have a significant financial impact to the trust service provider, with considerable administrative burden, when the provider has thousands of clients, in addition to the potential impact in terms of reputation.

SECTION 3

Qualified trust services

[Supervision of qualified trust service providers]

Article 20

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in

this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. The Commission may, by means of implementing acts, establish reference number of the following standards:

(a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;
(b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Art. 20 of the Regulation is applicable to the supervision of qualified trust service providers, in the course of their activities. Again, implementing acts may be adopted by the Commission in the context of this provision (pursuant to art. 20 (4) of the Regulation) but, at the time of writing, this had not occurred yet.

2. Audit every twenty-four months. Before the initiation of a qualified trust service, any provider shall be subject to an audit made by a 'conformity assessment body', that shall issue a 'conformity assessment report', submitted to the supervisory body (*see* art. 21 of the Regulation). The 'conformity assessment body' is defined by art. 3 (18) as 'a body defined in point 13 of art. 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides'. It is essential that, 'when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes' (recital 44). Regularly, i.e. every twenty-four months at least, a new audit shall be performed by a conformity assessment body, pursuant to art. 20 (1) of the Regulation, at the expense of the qualified trust service

provider. Its purpose is 'to confirm that that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation'. The report is then submitted to the supervisory body (within three working days after reception by the provider).

3. Audit at the request of (or by) the supervisory body. Within the twenty-four months period, the supervisory body is entitled to request the audit of qualified trust service provider, at its own cost, by a conformity assessment body (art. 20 (2) of the Regulation). Any user or competent public authority (the data protection authority, for instance) may notify the supervisory body of practices that are (potentially) non-compliant with the applicable framework. Following notification, the supervisory body should take measures without undue delay, in order to confirm the failure and ask for remedies accordingly. Such ad hoc conformity assessment report can however not be requested abusively. Recital 43 of the Regulation prescribes in this context that, 'whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment'. Cooperation with the competent data protection authority is also regulated: results of the audit must be communicated to it, when personal data protection rules appear to have been breached.

4. Penalties in case of failure to fulfil the requirements of the Regulation. As stated above, art. 16 of the Regulation states that Member States shall lay down effective, proportionate and dissuasive penalties, in case of infringements to the Regulation. A specific penalty – probably the most dissuasive – is also included in art. 20 (3) of the Regulation. The supervisory body is indeed entitled to withdraw the qualified status of a provider or of the affected service it provides. This could be the case where 'the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body'. The decision of the supervisory body must be taken with regard to various criterions and, in particular, 'the extent, duration and consequence of that failure'. In case of withdrawal of the authorisation, information shall be given to the trust service provider and to the body responsible for establishing, maintaining and publishing national trusted lists (*see* art. 22 (3) of the Regulation), so that such lists can be updated.

[Initiation of a qualified trust service]

Article 21

1. Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

4. The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Art. 3 (1) of the Directive 1999/93/EC on electronic signatures, into force until 1 July 2016, stated that 'Member States shall not make the provision of certification services subject to prior authorisation'. A different process is implemented by the eIDAS Regulation: prior authorisation shall be granted by the competent supervisory body so that a provider can be considered as trust service provider and further provides trust services. This initiation process is described by art. 21 of the Regulation. Implementing acts may be adopted by the Commission in the context of this provision (*see* art. 21 (4) of the regulation), but, at the time of writing, it has not occurred yet. It must also be pointed out that, following recital 45, 'preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services'.

2. Prior authorisation (paras 1–4). No qualified trust service shall be provided before the qualified status is indicated in the trusted list referred to in art. 22 (1) of the Regulation (art. 21 (3) of the Regulation). This indication can only be made when the supervisory decided to grant the qualified status to the provider and its services, in accordance with art. 21 (2) of the Regulation. The supervisory body shall decide taking into account the conformity assessment report issued by the conformity assessment body. Normally, the supervisory body will follow the conclusion of the report issued by the conformity assessment body, that took the time (and the responsibility) to assess carefully the applicable requirements of the eIDAS Regulation, in line the technical standards, while auditing the future provider. This report must be submitted to the

competent supervisory body, together with the notification of the trust service provider's intention to start qualified trust services (art. 21 (1) of the Regulation). The purpose of the prior assessment made by the supervisory body is to verify whether the trust services to be provided are compliant with the provisions of the Regulation. If so, the trust service provider and its relevant trust services shall be granted qualified status and information in this sense shall be given to the competent body referred to in art. 22 (3) of the Regulation, so that it is mentioned on the trusted list. From the notification, until the communication to the above-mentioned body for the update of the trusted list, no more than three months should normally occur. There is however no penalty, should this deadline not be respected. The supervisory is solely committed to inform the trust service provider on the reasons of the delay and the period within which the verification has to be concluded.

[Trusted lists]

Article 22

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Trust will never occur without transparency and the publicity of key information (*see* recital 46). Citizen, business and public authorities must indeed be entitled to know easily, and with a high level of reliability, which trust service providers are qualified, as well as the trust services they provided. Information must also be made available in a form suitable for automated processing. For this reason, art. 22 of the Regulation prescribes the establishment of trusted lists, both at the national level and at the EU level. Pursuant to art. 22 (5) of the Regulation, an implementing act must be adopted by the Commission in the context of this provision, by 18 September 2015. This is the Commission implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant

to art. 22 (5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235 of 9 September 2015, pp. 26–36).

2. Publication at the national level and at the EU level. Trusted lists shall first be established, maintained and published at the national level, by the Member States (more precisely a specific body appointed by them, usually the supervisory body), with regard to the trust service providers for which they are responsible (art. 22 (1) of the Regulation). Information must be given on the qualified trust service provider and on the qualified trust services provided by them. Such trusted list must be electronically signed or sealed and made available in a form suitable for electronic processing (art. 22 (2) of the Regulation). Relevant information on the competent body in the Member States and on the trusted lists must be communicated to the Commission (art. 22 (3) of the Regulation). The Commission will further 'make available to the public through a secure channel, the information referred to in para. 3 in electronically signed or sealed form suitable for automated processing' (art. 22 (4) of the Regulation). Such information is available on https://webgate.ec.europa.eu/tl-browser/#/.

[EU trust mark for qualified trust services]

Article 23

> **1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.**
>
> **2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.**
>
> **3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).**

1. General. Citizen, business and public authorities must easily know which trust service providers and which services are qualified or not. Trust service providers, who have gone through a long, complex and expensive process in order to get the status of qualified trust service provider, must be entitled to publish their status and communicate this to their customers and prospects, for business purposes. In this respect, a trust mark was created at the EU level (*see* Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services, OJ L 128 of 23 May 2015, pp. 13–15). As soon as the qualified status is indicated in the trusted list established at the national level, such EU

trust mark can be used by the providers, provided that a link to the relevant trust list is made available on their website.

[Requirements for qualified trust service providers]

Article 24

> **1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.**
>
> **The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:**
>
> **(a) by the physical presence of the natural person or of an authorised representative of the legal person; or**
> **(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or**
> **(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or**
> **(d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.**
>
> **2. A qualified trust service provider providing qualified trust services shall:**
>
> **(a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;**
> **(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;**
> **(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;**

(d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;
(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;
(f) use trustworthy systems to store data provided to it, in a verifiable form so that:
  (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
  (ii) only authorised persons can make entries and changes to the stored data,
  (iii) the data can be checked for authenticity;
(g) take appropriate measures against forgery and theft of data;
(h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;
(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);
(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;
(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Qualified trust services – and their providers – are subject to more stringent rules than the non-qualified trust services – and the non-qualified trust service providers. Art. 24 of the eIDAS Regulation lays down some of the rules that only apply

to the qualified trust service providers. They deal with the identification of the person to whom a qualified certificate is issued, the main requirements applicable to the providers, related to their legal, technical and financial capacity, as well as with the revocation of the certificates. Implementing acts may be adopted by the Commission in the context of this provision (pursuant to art. 24 (5) of the Regulation). At the time of writing, this had not occurred yet.

2. Identification of the natural or legal person to whom the qualified certificate is issued. A certificate for an electronic signature or electronic seal is an electronic attestation that at least confirms the name (or the pseudonym, should it be a natural person) of that person (*see* art. 3 (14) and 3 (29) for the definitions of certificate for electronic signature and for electronic seal). With regard to the legal effects granted to the qualified trust services, the identification of the person to whom the certificate is issued by the trust service providers must be carried out with a high level of certainty. For that purpose, art. 24 (1) of the Regulation requires the qualified trust service provider to verify, by itself or with the help of a third party, the identity and, if applicable, any specific attributes of the person – either natural or legal – to whom the qualified certificate is issued (and before such issuance). Four means of verification are mentioned in art. 24 (1), being agreed that verification must be performed in accordance with the applicable national laws. The first means is the 'physical presence of the natural person or of an authorised representative of the legal person.' (a). Physical presence is the most traditional method of identification: the correlation of the picture of the identity card or the passport with the physical person present before the trust service provider will normally grant a high level of certainty regarding the identity of such natural person. Such means of identification cannot be implemented remotely or by electronic means. The second (b) and third (c) means of identification aim at addressing such issue. The starting point is that the verification of the identity of the person will also occur by physical presence, since it is a pre-requirement of both means. However, identification can occur 'remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in art. 8 with regard to the assurance levels "substantial" or "high"'. A relationship is established between Chapter II of the Regulation, on 'Electronic Identification' (*see* above for detailed comments of the relevant provisions), and Chapter III, on 'Trust Services'. The other means, mentioned under (c), is pretty obvious: it refers to the qualified electronic signature or the qualified electronic seal, issued in compliance with the provision of the Regulation and, especially, the requirements of art. 24 (1), (a) or (b). The last means (d) remains undetermined at this stage: it refers to 'other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body'. With such methods, the physical presence of the person is not required. This

other mean shall however provide equivalent assurance in terms of reliability. Other identification methods could be functionally equivalent to the verification by physical presence. Such equivalence must be confirmed by a conformity assessment body, that will be accountable for such statement.

3. Technical, legal, organisational and financial capacity of the qualified trust service provider. Art. 24 (2) lays down eleven main requirements to be met by the qualified trust service provider with regard to its technical, legal organizational and financial capacity and skills. From a technical point of view, the requirements aim at ensuring the trustworthiness of the systems and products, in order to guaranty their integrity (*see* under (e) – trustworthy systems and products protected against modification), confidentiality (*see* under (f) – requirements for retrieval of data, changes du stored data, authenticity of data – and (g) – measures against forgery and theft of data) and sustainability of the data (*see* under (h) – data recorded for an appropriate period of time – and (i) – up-to-date termination plan to ensure continuity of service), especially in case of termination of the activities of the provider. Special requirements apply to the information to be provided to the company or person seeking to use the qualified trust service. The trust service provider must provide information about the services and the processing of personal, prior to entering into the contract with the customer. From a legal perspective, this triggers the requirements in contract law, of acceptance, by the customer, of Terms and Conditions (*see* under d), whether it concerns the contract or a privacy policy (*see* under j). Financial requirements are indicated under (c), stating that 'with regard to the risk of liability for damages in accordance with art. 13, [the provider shall] maintain sufficient financial resources and/ appropriate liability insurance, in accordance with national law'. From an organizational point of view, the provider shall employ staff and/or the subcontractor with necessary expertise, reliability, experience and qualifications (*see* under b). Attention must finally be paid to the requirement under (a) – information duty to the supervisory body, in case of modification to the provision of qualified trust services or intention to cease the activities – and under (k) establishment of an up-to-date data base for the qualified certificates (if applicable).

4. Revocation of the certificates. As already mentioned, certificates play a key role in the context of trust services. For various reasons – death of the natural person, termination of the legal person, lack of confidentiality, theft of data, etc. – a certificate can be revoked by the trust service provider. With regard to qualified trust service provider, art. 24 (3) of the eIDAS Regulation prescribes to register such revocation in any case within twenty-four hours after the receipt of the request. In addition, information about the validity or revocation of the certificates shall be provided to any relying party, free of charge and in an automated manner (*see* art. 24 (4) of the Regulation).

CHAPTER III

TRUST SERVICES

SECTION 4

Electronic signatures

[Legal effects of electronic signatures]

Article 25

> **1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.**
>
> **2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.**
>
> **3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.**

1. General. Art. 25 reformulates, in clearer wording, some of the principles that were already established in Directive 1999/93/EC. The eIDAS Regulation remains silent on what should be understood from the act of signing, as well as the functions that have to be fulfilled by an electronic signature. It is consequently something to be determined at national level. For instance, in French civil law, the handwritten signature identifies its user and shows its adherence to the signed act (*see* art. 1367 of the French Civil Code). As for an electronic signature, it is supposed to guarantee the link between the act and the signatory, as well as its identity – this matches the functions recognized to the handwritten signature –, and the integrity of the document – which is much more disputable since the integrity is not a function of the handwritten signature.

2. Legal effects applicable to both qualified and non-qualified electronic signatures. (a) The principle of non-discrimination. The basic legal effect that applies to every electronic signature – and this also applies to other trust services (*see* below) – is the principle of non-discrimination. This principle implies that a signature cannot be denied any legal effect nor admissibility as evidence on the sole basis that it was made in electronic format or that it does not comply with the conditions of a qualified signature. Attention should be paid to the fact that non-discrimination principle does not mean that the electronic signature will be deemed equivalent to a handwritten signature. In order for an electronic signature to be considered equivalent to a physical one, a second step must be added to the reasoning. This second step consists in the demonstration that the electronic signature achieves each function fulfilled by the handwritten signature and/or enumerated by the legislator or identified by the judge or any other person that has to give an interpretation. **(b) Double aspect.** The non-discrimination principle applies at two levels. It applies to non-qualified services in comparison with qualified services. Through the application of the principle at this

level, the European legislator recognizes that there is a market for qualified services and one for non-qualified services. Qualified services imply heavier conditions to be met by the trust service provider. Consequently, this brings costs for the customer. Taking into account the cost aspects, it is sometimes sufficient to resort to a non-qualified service instead of a qualified one. Moreover, the principle applies to an electronic process and the same process in a paper-based environment. The application of the non-discrimination principle at this level aims at promoting the use of information and communication technologies – which is one of the main purposes of the eIDAS Regulation –, as it would be too easy for a judge to diminish the effectiveness of the Regulation by just ruling out a process on the sole basis that it is electronic.

3. Legal effects applicable to qualified electronic signatures. The added value of using a qualified electronic signature compared to a non-qualified signature lies in the extra-legal effects that are attached to it. **(a) Principle of legal equivalency.** A qualified electronic signature benefits from a principle known as 'legal equivalency' This principle entails that such an electronic signature will be considered equivalent to the handwritten signature as regards the legal effect they are recognized. This principle reduces the margin of appreciation by a court. Unless counterevidence is submitted, the court will be required to regard the electronic process as an equivalent to the physical one. In the event of a dispute as to the validity of an electronic signature, the user of a qualified signature service will be exempted from the burden of evidence rules. The harmonization does not go further than establishing equivalent effects. The eIDAS Regulation leaves it to the national legislator to determine which specific functions and legal effects are attached to physical signatures and, consequently, which functions must be fulfilled by qualified electronic signatures. In arts 35 and 41 of the Regulation, it will be shown that a similar mechanism applies to qualified electronic seals and stamps. However, this application is not as far-reaching as the principle of equivalence. **(b) Mutual recognition clause.** Besides the principle of legal equivalency, another consequence of the utilization of a qualified electronic signature is the application of the mutual recognition clause. If a qualified electronic signature is produced in a Member State, it is compulsory for the other Member States to recognize it and to derive all relevant legal effects from such a qualified trust service. This clause aims at facilitating the cross-border provision of services as well as enabling businesses to operate on a cross-border basis, as stated in recital 9. As for the non-qualified signatures, although they do not benefit from the mutual recognition clause provided for in art. 25 (3), they still fall under art. 4 of the Regulation which establishes the principle of internal market.

[Requirements for advanced electronic signatures]

Article 26

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

1. General. As mentioned, the eIDAS Regulation provides for three types of electronic signatures. Apart from the case of electronic signatures in public services (*see* art. 27 and its Commentary), the Regulation does not distinguish between 'simple' and 'advanced' electronic signatures when it comes to the legal effects that are derived therefrom. In practice, however, it is likely that a court will be inclined to recognize the probative value of an advanced electronic signature, considering the higher reliability that is attached to the procedures used for those signatures, in comparison with a simple electronic signature. This article establishes a third category of electronic signature: the advanced electronic signature. Although it might be interpreted as inducing more complexity in a field that is already inherently complicated, the existence of this third category of electronic signature is justified in recital 50. This recital observes that different formats are already used by competent authorities in Member States, making it necessary 'to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically'.

2. Four requirements. Art. 26 provides for four requirements, which aim at guaranteeing the respect of the handwritten signature's functions, and ensuring a high level of security. The fourth condition also implies that the electronic signature must fulfil a function of integrity of the signed document, as any subsequent change in the signed data must be detectable (one could discuss that such function is also achieved by the handwritten signature). For the most part, the four requirements set out in art. 26 are identical to the ones that were provided for in the Directive 1999/93. There is, however, a change in the third condition. Art. 2 (2) sub-para. (c), of the Directive required that the advanced electronic signature should be 'created using means that the signatory can maintain under his sole control'. This wording meant that the user had to control the whole ecosystem in which the advanced electronic signature was created. Moreover, the user had to take security measures in order to make sure that the signature was maintained under his exclusive supervision. The Regulation replaced this requirement from the Directive with the following wording: 'it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control'. Under this provision, the user only has to keep the use of the signature under his sole control, with a high level of confidence. The signatory is therefore allowed to resort to a trust service provider for the creation of his or her signature. As it is unrealistic to require that an electronic signature remains completely under the control of the user, this is a welcome change.

[Electronic signatures in public services]

Article 27

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Art. 27 compels Member States to recognize advanced electronic signatures in the situations and subject to the fulfilment of several conditions – defined in the Commission's implementing acts (para. 5). This provision covers the hypothesis in which a Member State requires resorting to an advanced electronic signature – whether based on a qualified certificate (art. 27 (2) or not (art. 27 (1)) – in order to access an online service offered by a public sector body or on behalf of a public sector body. In this context, the Member State is compelled to recognize an electronic signature that is either of the same category or of a superior category. Para. 3 logically prevents Member States to require an electronic signature that presents a higher security level than a qualified electronic signature for the cross-border access to their online public services.

2. A fourth category of electronic signature? This article raises questions as to whether it did or did not establish a fourth category of electronic signature. It concerns the advanced electronic signature based on a qualified certificate. One may wonder if such an electronic signature should not simply be called a qualified electronic

signature. It seems that this hybrid category might be the result of a compromise between the Member States, as in some of them, access to online public services is subject to utilization of an advanced electronic signature based on a qualified certificate, but not necessarily created with a qualified electronic signature creation device. This is outlined in recital 50: 'competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically', which makes it 'necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically.'

3. Measures to be adopted by the Commission (paras 4 and 5). Para. 5 requires the Commission to adopt implementing acts in order to define formats which can be used as reference for advanced electronic signature, or reference methods where other formats are used. In this regard, the Commission adopted on 8 September 2015 the implementing Decision (EU) 2015/1506 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to arts 27 (5) and 37 (5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market OJ L 235, 9 September 2015. Para. 4 provides that the Commission can establish also reference numbers of standards for advanced electronic signatures, the conformity to which gives rise to a presumption of compliance with all requirements for advanced electronic signatures (art. 26) and for their recognition (art. 27 (1) and (2)). These requirements can be found in the Commission implementing Decision (EU) 2015/1506 (*see also* the Connecting Europe Facility (CEF) website: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-Signature+standards).

[Qualified certificates for electronic signatures]

Article 28

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Art. 28 specifies the rules governing qualified certificates for electronic signatures. Pursuant to art. 3 (12), a qualified electronic signature is 'an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures'. Therefore, what distinguishes the qualified electronic signature from the advanced electronic signature is the observance of two additional mandatory requirements (which add up to the requirements provided for in 26 of the Regulation as regards advanced electronic signatures). First, the electronic signature must be created using a qualified electronic signature creation device (art. 30 of the Regulation). Second, the electronic signature must be based on a qualified certificate for electronic signatures. The Commission has the possibility to adopt implementing acts in order to set out reference numbers of standards for qualified certificates for electronic signature. Respect of these standards gives rise to a presumption of compliance with the requirements laid down in Annex I.

2. Exhaustive list of requirements. The conditions to be met by qualified certificates are listed in Annex I of the Regulation (para. 1). Annex I consists of a list of information that shall be contained in qualified certificates and which help guaranteeing the security of the signed data. This information covers various aspects of the qualified electronic signature including, but not limited to, an indication that the certificate has been issued as a qualified certificate for electronic signature, information about the qualified trust service provider, name or pseudonym of the signatory, and information about the certificate's validity period. The signatory is allowed to use a pseudonym, as was already the case in the Directive (art. 8, para. 3 of Directive 1999/93/EC). If the signatory uses this option, specific mention must be made thereof. The trust service provider must be able to communicate the identification data at the request of the authorities (recital 33 and art. 32, e) of the Regulation). The list in Annex I is exhaustive. The Member States cannot set additional mandatory requirements (para. 2). This contributes to achieving interoperability and cross-border recognition of qualified certificates, which is necessary for cross-border recognition of qualified electronic signatures (recital 54). However, it remains possible to introduce additional specific attributes at national level, as long as those attributes are not mandatory and do not affect interoperability and cross-border recognition (para. 3).

3. Revocation and suspension (paras 4 and 5). A certificate can be revoked or suspended. The first hypothesis – a typical example being the decease of the signatory

– is dealt with in para. 4. Para. 4 provides that, when a certificate has been revoked, it loses its validity from the moment of revocation. It is important to note that such an operation is irreversible and a revoked certificate can never be reactivated. The qualified trust service provider who decides to revoke a certificate must register the operation and publish the revocation status of the certificate within twenty-four hours from the receipt of the request. As for suspension (para. 5), Member States benefit from some leeway, as they can lay down the national rules on temporary suspension of qualified certificates for electronic signatures. Their margin of maneuver is framed by two conditions. The first one holds in the effect of the suspension: suspension of the qualified certificate implies suspension of its validity during the period of suspension. The certificate shall regain its validity at the end of the suspension. The second condition consists of an information duty. The certificate database must indicate the suspension period and the suspension status must be visible for the duration of the suspension from the service providing information on the status of the certificate. As highlighted by recital 53, this is a matter of legal certainty.

[Requirements for qualified electronic signature creation devices]

Article 29

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Out of the three categories of electronic signatures, the qualified electronic signature demonstrates the highest degree of reliability from the technical point of view. This is the result of a number of requirements that must be met as regards every aspect of the qualified electronic signature – its creation, its validation and its preservation. Art. 29 refers to Annex II, which contains four requirements applying to qualified electronic signature creation devices. The first requirement calls for the use of appropriate technical and procedural means, in order to ensure, at least, confidentiality of the electronic signature creation data, uniqueness of the electronic signature creation data, protection against forgery and protection of the electronic signature creation data against the use by illegitimate persons. The second requirement relates to the signed data. These must not be altered by the qualified electronic signature creation devices, nor can they be invisible to the signatory prior to signing. The third requirement provides that only a qualified service provider can generate or manage electronic signature creation data on behalf of the signatory. The fourth requirement regulates the duplication of the electronic signature creation data by the qualified service provider for back-up purposes. The Commission can also lay down reference

numbers of standards for qualified electronic signature creation devices which will constitute the basis for a presumption of compliance with the requirements of Annex II.

[Certification of qualified electronic signature creation devices]

Article 30

> **1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.**
>
> **2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.**
>
> **3. The certification referred to in paragraph 1 shall be based on one of the following:**
>
> **(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or**
> **(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.**
>
> **The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).**
>
> **4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.**

1. General. Art. 30 provides for a certification mechanism based on a control designed to assess the conformity of electronic signature creation devices to the requirements laid down in Annex II. The control process shall be carried out by private or public bodies, designated by the Member States (para. 1). In this regard, Member States are subjected to an obligation of information that implies notification to the Commission of the names and addresses of the public or private body that is responsible for the control. The Commission then makes that information available to other Member States (para. 2).

2. Two options for certification (para. 3). The certification is either based on a security evaluation process corresponding to the standards set out by the Commission (para. 3, a)), or another process which uses comparable security levels (para. 3, b)). This alternative process must be notified to the Commission and can only be used as

long as there are no standards established by the Commission, or when a security evaluation process is ongoing. The Commission did adopt the standards mentioned in point a) in the Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to arts 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[Publication of a list of certified qualified electronic signature creation devices]

Article 31

> **1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.**
>
> **2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.**
>
> **3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).**

1. General. Para. 1 provides that once a qualified electronic signature creation device has been certified, the Member State must, within one month after the certification is completed, notify information about this device to the Commission. In case of cancellation of a qualified electronic signature creation device, the Commission must also be informed by the Member State. This transfer of information shall allow the Commission to establish, publish and maintain a list of certified qualified electronic signature creation devices (para. 2). This will allow for a centralization of information about all the qualified electronic creation devices which have met every requirement set out in art. 30 (1). The Commission can regulate the way notifications are carried out by defining formats and procedures applicable thereto (para. 3).

[Requirements for the validation of qualified electronic signatures]

Article 32

> **1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:**
>
> **(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;**
> **(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;**

(c) the signature validation data corresponds to the data provided to the relying party;
(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
(f) the electronic signature was created by a qualified electronic signature creation device;
(g) the integrity of the signed data has not been compromised;
(h) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Validation is the process through which the electronic signature is verified and confirmed. When related to a qualified electronic signature, the validation process must comply with conditions listed in art. 32. Here again, in order to facilitate validation, the Commission may adopt implementing acts setting reference numbers of standards for the validation of qualified electronic signatures (para. 3). If the validation process corresponds to the standards, it generates a presumption according to which the validation was made in compliance with all the requirements related thereto.

2. Verification of the components of the qualified electronic signature (paras 1 and 2). Pursuant to recital 57, it is a matter of legal certainty 'to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation.' In this sense, art. 32 (1) lists a series of elements related to the requirements of the qualified electronic signature that are to be checked by the party taking care of the validation process. Thus, the party proceeding to the validation must verify compliance of the certificate with Annex 1, the issuance by a qualified trust service provider and validity at the time of signing, the validation data, the data uniquely representing the signatory, the use of a qualified electronic signature creation device, the integrity of the signed data, and compliance with the conditions applying to the advanced signature at the time of signing. The relying party must also receive a clear indication if a pseudonym was used at the time of signing (para. 1, e)). Validation should be carried out through a system that will provide to the relying party the correct result of the validation process. Moreover, the system must be of such a nature that the relying party will be able to detect any issues as to the security attached to the qualified electronic signature (para. 2).

[Qualified validation service for qualified electronic signatures]

Article 33

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

(a) provides validation in compliance with Article 32(1); and
(b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. A qualified validation service for electronic signatures is provided by a qualified trust service provider. The qualified trust service provider must proceed to the validation process in compliance with the requirements listed in art. 32, meaning that every enumerated element must be verified (para. 1, a)). The trust service provider must also ensure that the result of the validation process is made available to relying parties in an automated manner. This communication shall be reliable and efficient and contain either the advanced electronic signature of the service provider – if it is a natural person –, or its advanced electronic seal – if it is a legal person. The Commission may establish reference numbers of standards for qualified validation service. If these standards are complied with, it is presumed that all requirements set out by para. 1 are met.

[Qualified preservation service for qualified electronic signatures]

Article 34

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. This provision merely indicates that a qualified preservation service for qualified electronic signatures has to be delivered by a qualified trust service provider. Additionally, this provider must make use of tools that will be suitable in maintaining the trustworthiness of the qualified electronic signature beyond the technological validity period. Long-term preservation of information linked to electronic signatures is of utmost importance in order to guarantee that electronic signatures will remain valid and continue to produce legal effects independently from technical evolution (recital 61). Para. 2 confers a prerogative to the Commission, which has the possibility to take implementing acts in order to establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. These standards are at the basis of a presumption of fulfilment of the requirements laid down in para. 1 if they are complied with.

2. A missed opportunity? This provision seems to contain the premises of an electronic archiving regime. One may regret that the Regulation does not provide for a full-fledged electronic archiving regime, as it represented a real opportunity to build a set of rules regarding this issue at the European level.

SECTION 5

Electronic seals

[Legal effects of electronic seals]

Article 35

> **1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.**
>
> **2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.**
>
> **3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.**

1. General. The electronic seal is an innovation in the eIDAS Regulation. It can be compared to an electronic signature, as the means used to create it are identical, the first main difference being that a seal is designed to be used by a legal entity. This is apparent from the formulation of recital 59: 'Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.' In other words, the electronic seal guarantees the link between the electronic document and the legal entity. Moreover, as stated in recital 65, any digital asset of the legal person can be authenticated by an electronic seal. The second difference lies in the effects associated respectively to electronic signatures and seals. The electronic signature has the capacity to bind the physical person, while the electronic seal only guarantees the origin and integrity of the electronic documents

issued by the legal entity. For instance, the electronic seal can be used in order to demonstrate that certain software originates from a legal entity and has not been altered. However, the legal entity will not be able to use the electronic seal to sign a document. This does not prevent the Member States to provide otherwise. For example, making use of this possibility, the Belgian legislator has given similar legal effects to the electronic seal as those given to the electronic signature (*see* art. XII.25 of the Belgian Code of Economic Law).

2. Legal effect applicable to both qualified and non-qualified electronic seals. As it is the case with electronic signatures, electronic seals – qualified and non-qualified – cannot be ruled out of legal proceedings nor can they be denied legal effect for the sole reason that the seal appears in electronic format (principle of non-discrimination). The sole implication of this is that the judge will have to take the seal into account.

3. Legal effect applicable to qualified electronic seals. A legal presumption applies to qualified electronic seals: the integrity of the data and the correctness of the origin of that data are presumed. Similarly to what is established for a qualified signature, the user of a qualified electronic seal will be exempted from the burden of evidence rules. Second of all, a qualified electronic seal has to be recognized as such, with all the legal effects it conveys, in all Member States. This recognition therefore contributes to the smooth functioning of the internal market.

[Requirements for advanced electronic seals]

Article 36

> **An advanced electronic seal shall meet the following requirements:**
>
> **(a) it is uniquely linked to the creator of the seal;**
> **(b) it is capable of identifying the creator of the seal;**
> **(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and**
> **(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.**

1. General. The requirements to be fulfilled by the advanced electronic seal are identical to the ones applicable to the advanced electronic signature (art. 26). Accordingly, the advanced electronic seal must, first of all, be uniquely linked to the creator of the seal. As is the case for the advanced electronic signature, one seal can only be linked to one user – a legal person in this case. Second, from the electronic seal, it must be possible to identify the legal person it is linked to. Third, the creation of the electronic seal must be made with data which is used under the control of the creator, with a high level of confidence. Fourth, any subsequent change in the data must be detectable thanks to the seal affixed thereto. This last condition is a translation of one of the function of the electronic seal, namely the function of integrity of the data produced by the legal person.

2. No specific legal effect. Besides the effect normally recognized to any electronic seal, namely the non-discrimination principle (art. 35 (1)), and under reservation of the recognition provided for in art. 37, when a Member State requires an electronic seal in order to access an online public service, there is no real additional effect specified by the Regulation for the use of an advanced electronic seal. However, it can be expected, considering the requirements that must be fulfilled by electronic advanced seals, that the judge will be likely to consider that such an electronic process has the capacity to guarantee the origin and integrity of the data it is linked to. This will have to be verified by the practice of the national judges.

[Electronic seals in public services]

Article 37

> 1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
>
> 2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
>
> 3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.
>
> 4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).
>
> 5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. This article is tantamount to art. 27, which provides for the same rule as regards electronic signatures. As a reminder, when a Member State requires an advanced electronic seal, whether based on a qualified certificate (para. 2) or not (para. 1), for access to an online public service, it is compelled to accept the electronic seal showing an equivalent or superior level or security. For example, if the access to a French public service requires the use of an advanced electronic seal in order to have access to this service, it shall be possible for a Belgian legal person to use either an

advanced electronic seal, or and advanced electronic seal based on a qualified certificate, or a qualified electronic seal. This is however subject to a condition of compliance with the formats or methods which must be provided for by the Commission in its implementing acts (para. 5). These are to be found in the Commission Implementing Decision (EU) 2015/1506 of 8 September 2015, alongside the formats and methods of advanced electronic signatures. Similarly to what was done as regards the electronic signature, this article seems to introduce a fourth type of electronic seal, namely the advanced electronic seal based on a qualified certificate. This seemingly additional category is probably intended to accommodate technical solutions that were already used in some Member States that required advanced electronic seals based on qualified certificates, but not created through a qualified seal creation device. Paragraph 3 forbids the Member States to isolate themselves in excessively high security requirements. Therefore, Member States cannot request that a legal person uses an electronic seal that shows a security level superior to a qualified electronic seal for cross-border access to an online public service. Under para. 4, the Commission may establish reference numbers of standards for advanced electronic seals. Observance with these standards would give rise to a presumption that all relevant requirements are met.

[Qualified certificates for electronic seals]

Article 38

> 1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.
>
> 2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.
>
> 3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.
>
> 4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
>
> 5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:
>
> (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;
> (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
>
> 6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. Like the qualified electronic signature, the qualified electronic seal must include two additional elements compared to the advanced electronic process. First, the qualified electronic seal must be created using a qualified electronic seal creation device that has to comply with the terms of Annex II. Second, the qualified electronic seal must be based on a qualified certificate issued by a qualified trust service provider. Para. 6 provides for the possibility left to the Commission to adopt implementing acts setting out reference numbers of standards for qualified certificates for electronic seals. Compliance to such standards would give rise to a presumption according to which all the requirements applying to the qualified certificate are met.

2. Criteria set out in Annex III. The qualified certificate must fulfil the requirements set out in Annex III, which are designed to guarantee the security of data to the third parties who receive them. The information to be provided covers the identity of the legal person who creates the seal, information about the qualified trust service provider issuing the qualified certificate and the duration of the qualified certificate's validity period. recital 60 underlines the importance of making it possible to identify the natural person representing the legal person that is the holder of the qualified certificate for the electronic seal. In this sense, 'Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures' in order to allow the identification.

3. Period of validity. Qualified certificates for electronic seals are valid for a certain period. Once this period is expired, seal creation data become unusable for the legal person. It is therefore important to ensure that the validity period matches the duration of the mandate of the natural person using the electronic seal. In the same vein, special attention needs to be paid in the hypothesis of a change in the representation power of the legal person's mandatary during the period of validity of the qualified certificate for the electronic seal. In such a case, the qualified certificate should be revoked in order to avoid the development of an apparent situation contrary to the reality.

[Qualified electronic seal creation devices]

Article 39

> **1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.**
>
> **2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.**
>
> **3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.**

1. General. Art. 39 merely refers to arts 29–31 which regulates qualified electronic signature devices. We therefore refer to the Commentary of these articles.

[Validation and preservation of qualified electronic seals]

Article 40

> **Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.**

1. General. The validation process, as well as the preservation of the electronic seal obey the same principles as for the electronic signature. We therefore refer to the Commentaries of arts 32, 33 and 34.

SECTION 6

Electronic time stamps

[Legal effect of electronic time stamps]

Article 41

> **1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.**
>
> **2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.**
>
> **3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.**

1. General. Art. 41 of the eIDAS Regulation determines the legal effects of electronic time stamps. The principle of non-discrimination shall apply to both qualified and non-qualified electronic time stamps (art. 41 (1) of the Regulation). Furthermore, qualified electronic time stamp shall benefit from the presumption established in art. 41 (2) of the Regulation and from the international recognition consecrated in art. 41 (3). The structure and main rules provided by this article are similar to the corresponding articles on the legal effects of electronic signature, seal or registered delivery services. Such legal effects shall apply no matter the requirement of time stamp is prescribed for evidentiary purposes or as a requirement of validity for the legal act.

2. Legal effects applicable to both qualified and non-qualified electronic time stamps. The principle of non-discrimination is applicable to both qualified and non-qualified electronic time-stamps, with regard to the '*electronic v. paper*' dimension: such trust service cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form. Furthermore, the non-qualified electronic time stamp shall benefit from the principle of non-discrimination with regard to the '*qualified status v. non-qualified status*' dimension: such trust service cannot be denied legal effect and admissibility as evidence in legal

proceedings solely on the grounds that it does not meet the requirements of the qualified electronic time stamp. In both dimensions, it means that, in case of litigation, the competent jurisdiction shall not reject the trust service on this sole ground. Nevertheless, it does not mean that the trust service shall automatically benefit from full legal effects: for the qualified electronic time stamps, the requirements of art. 42 of the Regulation must be fulfilled and for the non-qualified electronic time stamps, the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound shall be demonstrated.

3. Legal effects applicable to qualified electronic time stamps. Qualified electronic time stamps are subject additional requirements (compared to non-qualified electronic time stamps) prescribed by Art. 42 of the Regulation. Should they be fulfilled, the following legal effects shall apply. (i) Pursuant to art. 13 of the Regulation, the burden of proof is on the trust service provider: it must indeed prove that the damages occurred without any intention or negligence in order to benefit from an exoneration of liability. (ii) A presumption is established by art. 41 (2) of the Regulation in the case of qualified electronic time stamps: the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound are indeed presumed. (iii) The third legal effects only applicable to the qualified electronic time stamp is related to its recognition, as such a qualified trust service, in all Member States (art. 41 (3) of the Regulation). It means that the qualified electronic time stamp issued by a provider established in Estonia shall benefit from all legal effects prescribed by the Regulation (presumption and liability) in all other Member States. Such recognition is necessary to achieve to goal of ensuring the proper functioning of the internal market.

[Requirements for qualified electronic time stamps]

Article 42

1. A qualified electronic time stamp shall meet the following requirements:

(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
(b) it is based on an accurate time source linked to Coordinated Universal Time; and
(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. In order to benefit from the legal effects granted to the qualified electronic time stamps, the parties relying thereon must be given a higher level of legal certainty

and the specific requirements laid down in art. 42 (1) of the eIDAS Regulation must be fulfilled. These requirements aim at ensuring that the functions expected from an electronic time stamp – accuracy of the time and date it indicated and integrity of the data to which time and date are bound – are achieved with a higher level of legal certainty. For these purposes, the service shall 'reasonably preclude the possibility of the data being changed undetectably' (a), be 'based on an accurate time source linked to Coordinated Universal Time' (b) and shall be signed 'using an advanced electronic signature or sealed with an electronic seal of the qualified trust service provider, or by some equivalent method' (c). Implementing acts may be adopted by the Commission in the context of this provision (*see* art. 42 (4) of the Regulation), in order to establish reference numbers of standards. At the time of writing, it has not occurred yet. However, it is very likely that such norms will be enacted since the compliance with such standards is considered to be a presumption of compliance with the requirements laid down in art. 42 (1) of the Regulation.

SECTION 7

Electronic registered delivery services

[Legal effect of an electronic registered delivery service]

Article 43

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

1. General. Art. 43 of the eIDAS Regulation determines the legal effects of data sent and received using an electronic registered delivery service. Both qualified and non-qualified electronic registered delivery services shall be subject to the principle of non-discrimination (art. 43 (1) of the Regulation) which can be derived from the wording in para. 1 – *see* under 2). Qualified electronic registered delivery service shall benefit from the presumption established in art. 43 (2) of the Regulation. The structure and main rules provided by this article are similar to the corresponding articles on the legal effects of electronic signature, seal or time stamps.

2. Legal effects applicable to both qualified and non-qualified electronic registered delivery service. The principle of non-discrimination applies both to qualified and non-qualified electronic registered delivery services: such trust service cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form (instead of 'paper form'). Furthermore, the

non-qualified electronic registered delivery service shall benefit from the principle with regard to the 'qualified status' dimension: data sent by and received from such trust service cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it does not meet the requirements of the qualified electronic registered delivery service. The foregoing means that, in case of litigation, the competent court may not reject the trust service on this sole ground. However, it does not mean that the trust service shall automatically benefit from full legal effect: for the qualified electronic time stamps, the requirements of art. 44 of the Regulation must be fulfilled and, for the non-qualified electronic registered delivery service, evidence must be submitted of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt.

3. Legal effects applicable to qualified electronic registered delivery services. In comparison with the non-qualified electronic registered delivery services, qualified electronic registered delivery services are subject to numerous and more stringent requirements. Accordingly, legal certainty for the parties relying thereon is higher. Pursuant to art. 13 of the Regulation, the burden of proof lies with the trust service provider: it must prove that the damages occurred without any intention or negligence in order to benefit from an exoneration of liability. Another presumption is established by art. 44 (2) of the Regulation: 'data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service'. Such functions are normally achieved by the 'paper' registered delivery services granting the higher level of legal certainty. Finally, and contrariwise to the other qualified trust services (electronic signatures, seals and time stamps), there is not any international recognition in all Member States for qualified electronic registered delivery services.

[Requirements for qualified electronic registered delivery services]

Article 34

1. Qualified electronic registered delivery services shall meet the following requirements:

(a) they are provided by one or more qualified trust service provider(s);
(b) they ensure with a high level of confidence the identification of the sender;
(c) they ensure the identification of the addressee before the delivery of the data;
(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. In order to benefit from the legal effects granted to the qualified electronic registered delivery services, ensuring to the relying parties a higher level of legal certainty, specific requirements laid down in art. 44 (1) of the Regulation must be fulfilled. The requirements aim at ensuring that the functions expected from an electronic registered delivery service – the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt – are achieved with a higher level of legal certainty. Requirements under letters (a) to (f) aim at identifying both the sender and the addressee and at ensuring the integrity of the data (with an advanced electronic signature or seal), as well as the date and time of sending and receiving (with a qualified electronic time stamp). Implementing acts may be adopted by the Commission in the context of this provision (*see* art. 44 (2) of the regulation), in order to establish reference numbers of standards for processes for sending and receiving data but, at the time of writing, it has not occurred yet. Such standards are necessary. Compliance with such standards shall be considered a presumption of compliance with the requirements laid down in art. 44 (1) of the Regulation.

SECTION 8

Website authentication

[Requirements for qualified certificates for website authentication]

Article 45

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

1. General. As stated in recital 67 of the Regulation, 'Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated'. The purpose of this specific trust service, without any equivalent in the 'paper' environment, is to prevent, as much as possible, the occurrence of cybercrimes and, in particular, phishing. Certificates for website authentication can be qualified or non-qualified. Art. 45 of the Regulation deals with qualified certificates. Art. 45 indicates that such certificates must fulfil the requirements of Annex IV. Annex IV aims at identifying the qualified trust service provider and the person to whom certificate is issued. Implementing acts may be adopted by the Commission in the context of this provision (*see* art. 45 (2) of the Regulation), in order to establish reference numbers of standards for qualified certificates for website authentication but, at the time of writing, it has not occurred yet. Such norms are necessary, since the compliance with such standards shall be considered as a presumption of compliance with the requirements laid down in Annex IV of the Regulation.

CHAPTER IV

ELECTRONIC DOCUMENTS

[Legal effects of electronic documents]

Article 46

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

1. General. The electronic document is defined in art. 3 (35) of the eIDAS Regulation. Art. 46 is laid down in a new chapter of the Regulation, as the electronic document does not constitute a trust service. This provision deals with the legal effects of electronic documents, with the consecration of the principle of non-discrimination, in its '*electronic v. paper*' dimension. It is prohibited to deny electronic documents legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in electronic form. It does not matter whether such document is prescribed or used for evidentiary purposes or as a validity requirement of the legal act. Consequently, the competent court cannot reject such document for the aforementioned reasons. It does not mean, however, that the electronic document shall automatically benefit from full legal effect: the party using the electronic document must demonstrate that the electronic process fulfills the functions expected from the corresponding formality in the paper context (for instance, a written form), in accordance with the applicable legal framework.

CHAPTER V

DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

[Exercise of the delegation]

Article 47

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.

3. The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

1. General. The Regulation addresses a number of predominantly technical issues. The stakeholders expect legal certainty, with regard to the standards and technical norms applicable to the trust services. For this purpose, delegated acts may (or shall) be adopted by the European Commission, in compliance with this art. 48 of the Regulation, especially to define technical standards.

[Committee procedure]

Article 48

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011..

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

1. General. This provision deals with the committee procedure, as regulated by the Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

CHAPTER VI

FINAL PROVISIONS

[Review]

Article 49

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.

In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

1. General. This provision deals with the review related to the application of the Regulation (no later than 1 July 2020, i.e. after four years). Special attention must be paid to possible modification of the scope of some provisions.

[Repeal]

Article 50

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.

2. References to the repealed Directive shall be construed as references to this Regulation.

1. General. From the application of the Regulation, on 1 July 2016, the Directive 1999/93/EC, who only dealt with electronic signature (topic now regulated by the Regulation), shall be repealed.

[Transitional measures]

Article 51

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.

3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.

4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

1. General. This provision establishes the transitional measures applicable to the qualified certificates issued to natural persons under Directive 1999/93/EC. The situation of the certification-service-provider issuing qualified certificates under Directive 1999/93/EC is also regulated, whether they submitted a conformity assessment report to the supervisory body no later than 1 July 2017.

[Entry into force]

Article 52

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. This Regulation shall apply from 1 July 2016, except for the following:

(a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;
(b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);
(c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).

3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.

4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

1. General. Most provisions of the Regulation are applicable from 1 July 2016. Others are applicable earlier or later, as detailed in the provision, so it is always necessary to verify per provision what it provides as regards entry into force.